Comprehensive Introduction to Linear Algebra

PART I - BASIC LINEAR ALGEBRA

Joel G. Broida

S. Gill Williamson

$$\begin{tikzcd}
N = \begin{bmatrix} [a_{11} & a_{12} & \dots & a_{1n}] \\ [a_{21} & a_{22} & \dots & a_{2n}] \\ \vdots & \vdots & \vdots & \vdots \\ [a_{m1} & a_{m2} & \dots & a_{mn}] \end{bmatrix} \arrow[r, bend left, leftrightarrow] & C = \begin{bmatrix} \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} & \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} & \begin{matrix} \dots \\ \dots \\ \vdots \\ \dots \end{matrix} & \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} \end{bmatrix}
\end{tikzcd}$$

Comprehensive Introduction to Linear Algebra

PART I - BASIC LINEAR ALGEBRA

Joel G. Broida
S. Gill Williamson

Preface (Part I)

This book, Part I - Basic Linear Algebra, covers Chapters 0 through 5 of the book *A Comprehensive Introduction to Linear Algebra* (Addison-Wesley, 1986), by Joel G. Broida and S. Gill Williamson. Chapters 0 and 1 are for review as needed. Chapters 2 through 5, supplemented by selections from Part II and Part III in this series, is suitable for a first course in linear algebra for upper division undergraduates. The original Preface (included here) gives other suggestions.

Preface (Parts I, II, III)

As a text, this book is intended for upper division undergraduate and beginning graduate students in mathematics, applied mathematics, and fields of science and engineering that rely heavily on mathematical methods. However, it has been organized with particular concern for workers in these diverse fields who want to review the subject of linear algebra. In other words, we have written a book which we hope will still be referred to long after any final exam is over. As a result, we have included far more material than can possibly be covered in a single semester or quarter. This accomplishes at least two things. First, it provides the basis for a wide range of possible courses that can be tailored to the needs of the student or the desire of the instructor. And second, it becomes much easier for the student to later learn the basics of several more advanced topics such as tensors and infinite-dimensional vector spaces from a point of view coherent with elementary linear algebra. Indeed, we hope that this text will be quite useful for self-study. Because of this, our proofs are extremely detailed and should allow the instructor extra time to work out exercises and provide additional examples if desired.

A major concern in writing this book has been to develop a text that addresses the exceptional diversity of the audience that needs to know something about the subject of linear algebra. Although seldom explicitly acknowledged, one of the central difficulties in teaching a linear algebra course to advanced students is that they have been exposed to the basic background material from many different sources and points of view. An experienced mathematician will see the essential equivalence of these points of view, but these same differences seem large and very formidable to the students. An engineering student for example, can waste an inordinate amount of time because of some trivial mathematical concept missing from their background. A mathematics student might have had a concept from a different point of view and not realize the equivalence of that point of view to the one currently required. Although such problems can arise in any advanced mathematics course, they seem to be particularly acute in linear algebra.

To address this problem of student diversity, we have written a very self-contained text by including a large amount of background material necessary for a more advanced understanding of linear algebra. The most elementary of this material constitutes Chapter 0, and some basic analysis is presented in three appendices. In addition, we present a thorough introduction to those aspects of abstract algebra, including groups, rings, fields and polynomials over fields, that relate directly to linear algebra. This material includes both points that may seem "trivial" as well as more advanced background material. While trivial points can be quickly skipped by the reader who knows them already, they can cause discouraging delays for some students if omitted. It is for this reason that we have tried to err on the side of over-explaining concepts, especially when these concepts appear in slightly altered forms. The more advanced reader can gloss over these details, but they are there for those who need them. We hope that more experienced mathematicians will forgive our repetitive justification of numerous facts throughout the text.

A glance at the Contents shows that we have covered those topics normally included in any linear algebra text although, as explained above, to a greater level of detail than other books. Where we differ significantly in content from most linear algebra texts however, is in our treatment of canonical forms (Chapter 8), tensors (Chapter 11), and infinite-dimensional vector spaces (Chapter 12). In particular, our treatment of the Jordan and rational canonical forms in Chapter 8 is based entirely on invariant factors and the

Smith normal form of a matrix. We feel this approach is well worth the effort required to learn it since the result is, at least conceptually, a constructive algorithm for computing the Jordan and rational forms of a matrix. However, later sections of the chapter tie together this approach with the more standard treatment in terms of cyclic subspaces. Chapter 11 presents the basic formalism of tensors as they are most commonly used by applied mathematicians, physicists and engineers. While most students first learn this material in a course on differential geometry, it is clear that virtually all the theory can be easily presented at this level, and the extension to differentiable manifolds then becomes only a technical exercise. Since this approach is all that most scientists ever need, we leave more general treatments to advanced courses on abstract algebra. Finally, Chapter 12 serves as an introduction to the theory of infinite-dimensional vector spaces. We felt it is desirable to give the student some idea of the problems associated with infinite-dimensional spaces and how they are to be handled. And in addition, physics students and others studying quantum mechanics should have some understanding of how linear operators and their adjoints are properly defined in a Hilbert space.

One major topic we have not treated at all is that of numerical methods. The main reason for this (other than that the book would have become too unwieldy) is that we feel at this level, the student who needs to know such techniques usually takes a separate course devoted entirely to the subject of numerical analysis. However, as a natural supplement to the present text, we suggest the very readable "Numerical Analysis" by I. Jacques and C. Judd (Chapman and Hall, 1987).

The problems in this text have been accumulated over 25 years of teaching the subject of linear algebra. The more of these problems that the students work the better. Be particularly wary of the attitude that assumes that some of these problems are "obvious" and need not be written out or precisely articulated. There are many surprises in the problems that will be missed from this approach! While these exercises are of varying degrees of difficulty, we have not distinguished any as being particularly difficult. However, the level of difficulty ranges from routine calculations that everyone reading this book should be able to complete, to some that will require a fair amount of thought from most students.

Because of the wide range of backgrounds, interests and goals of both students and instructors, there is little point in our recommending a particular course outline based on this book. We prefer instead to leave it up to each teacher individually to decide exactly what material should be covered to meet the needs of the students. While at least portions of the first seven chapters should be read in order, the remaining chapters are essentially independent of each other. Those sections that are essentially applications of previous concepts, or else are not necessary for the rest of the book are denoted by an asterisk (*).

Now for one last comment on our notation. We use the symbol ∎ to denote the end of a proof, and // to denote the end of an example. Sections are labeled in the format "Chapter.Section," and exercises are labeled in the format "Chapter.Section.Exercise." For example, Exercise 2.3.4 refers to Exercise 4 of Section 2.3, i.e., Section 3 of Chapter 2. Books listed in the bibliography are referred to by author and copyright date.

Contents (Part I,# II, III)

CHAPTER 0

Foundations

This text discusses the theory of finite–dimensional vector spaces in sufficient detail to enable the reader to understand and solve most linear algebra problems in mathematics and physics likely to be encountered outside of specialized research. In other words, we treat the general theory of determinants and matrices along with their relationship to linear transformations. Our approach will generally be rather abstract since we feel that most readers already have a reasonable amount of experience in visualizing vectors in three dimensions. Furthermore, we will not discuss any analytic geometry. Those readers who wish to learn something about this subject are referred to the books listed in the bibliography.

In this chapter, we briefly go through some elementary concepts from analysis dealing with numbers and functions. While most readers will probably be familiar with this material, it is worth summarizing the basic definitions that we will be using throughout this text, and thus ensure that everyone is on an equal footing to begin with. This has the additional advantage in that it also makes this text virtually self–contained and all the more useful for self–study. The reader should feel free to skim this chapter now, and return to certain sections if and when the need arises.

0.1 SETS

For our purposes, it suffices to assume that the concept of a set is intuitively clear, as is the notion of the set of integers. In other words, a **set** is a collection of objects, each of which is called a **point** or an **element** of the set. For example, the set of integers consists of the numbers 0, ± 1, ± 2, . . . and will be denoted by $\mathbb{Z}$. Furthermore, the set $\mathbb{Z}^+$ consisting of the numbers 1, 2, . . . will be called the set of **positive integers**, while the collection 0, 1, 2, . . . is called the set of **natural numbers** (or **nonnegative** integers). If m and $n \neq 0$ are integers, then the set of all numbers of the form m/n is called the set of **rational numbers**, and will be denoted by $\mathbb{Q}$. We shall shortly show that there exist real numbers not of this form. The most important sets of numbers that we shall be concerned with are the set $\mathbb{R}$ of real numbers and the set $\mathbb{C}$ of complex numbers (both of these sets will be discussed below).

If S and T are sets, then S is said to be a **subset** of T if every element of S is also an element of T, i.e., $x \in S$ implies $x \in T$. If in addition $S \neq T$, then S is said to be a **proper** subset of T. To denote the fact that S is a subset of T, we write $S \subset T$ (or sometimes $T \supset S$ in which case T is said to be a **superset** of S). Note that if $S \subset T$ and $T \subset S$, then $S = T$. This fact will be extremely useful in many proofs. The set containing no elements at all is called the **empty set** and will be denoted by $\varnothing$.

Next, consider the set of all elements which are members of T but not members of S. This defines the set denoted by $T - S$ and called the **complement** of S in T. (Many authors denote this set by $T \setminus S$, but we shall not use this notation.) In other words, $x \in T - S$ means that $x \in T$ but $x \notin S$. If (as is usually the case) the set T is understood and $S \subset T$, then we write the complement of S as S^c.

Example 0.1 Let us prove the useful fact that if $A, B \subset X$ with $A^c \subset B$, then it is true that $B^c \subset A$. To show this, we simply note that $x \in B^c$ implies $x \notin B$, which then implies $x \notin A^c$, and hence $x \in A$. This observation is quite useful in proving many identities involving sets. ∕∕

Now let $S_1, S_2, \ldots$ be a collection of sets. (Such a collection is called a **family** of sets.) For simplicity we write this collection as $\{S_i\}$, $i \in I$. The set I is called an **index set**, and is most frequently taken to be the set $\mathbb{Z}^+$. The **union** $\cup_{i \in I} S_i$ of the collection $\{S_i\}$ is the set of all elements that are members of at least one of the S_i. Since the index set is usually understood, we will simply write this as $\cup S_i$. In other words, we write

$$\cup S_i = \{x \colon x \in S_i \text{ for at least one } i \in I\} .$$

This notation will be used throughout this text, and is to be read as "the set of all x such that x is an element of S_i for at least one $i \in I$." Similarly, the **intersection** $\cap S_i$ of the S_i is given by

$$\cap S_i = \{x: x \in S_i \text{ for all } i \in I\} \ .$$

For example, if $S, T \subset X$, then $S - T = S \cap T^c$ where $T^c = X - T$. Furthermore, two sets S_1 and S_2 are said to be **disjoint** if $S_1 \cap S_2 = \varnothing$.

We now use these concepts to prove the extremely useful "**De Morgan Formulas**."

Theorem 0.1 Let $\{S_i\}$ be a family of subsets of some set T. Then

(a) $\cup {S_i}^c = (\cap S_i)^c$

(b) $\cap {S_i}^c = (\cup S_i)^c$

Proof (a) $x \in \cup {S_i}^c$ if and only if x is an element of some ${S_i}^c$, hence if and only if x is not an element of some S_i, hence if and only if x is not an element of $\cap S_i$, and therefore if and only if $x \in (\cap S_i)^c$.

(b) $x \in \cap {S_i}^c$ if and only if x is an element of every ${S_i}^c$, hence if and only if x is not an element of any S_i, and therefore if and only if $x \in (\cup S_i)^c$. ∎

While this may seem like a rather technical result, it is in fact directly useful not only in mathematics, but also in many engineering fields such as digital electronics where it may be used to simplify various logic circuits.

Finally, if $S_1, S_2, \dots, S_n$ is a collection of sets, we may form the (ordered) set of all n-tuples $(x_1, \dots, x_n)$ where each $x_i \in S_i$. This very useful set is denoted by $S_1 \times \cdots \times S_n$ and called the **Cartesian product** of the S_i.

Example 0.2 Probably the most common example of the Cartesian product is the plane $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Each point $\vec{x} \in \mathbb{R}^2$ has **coordinates** (x, y) where $x, y \in \mathbb{R}$. In order to facilitate the generalization to $\mathbb{R}^n$, we will generally write $\vec{x} = (x_1, x_2)$ or $\vec{x} = (x^1, x^2)$. This latter notation is used extensively in more advanced topics such as tensor analysis, and there is usually no confusion between writing the components of $\vec{x}$ as superscripts and their being interpreted as exponents (see Chapter 11). ∕∕

Exercises

1. Let A, B and C be sets. Prove that
   (a) $(A - B) \cap C = (A \cap C) - (B \cap C)$.
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
   (c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
   (d) $(A - B) - C = A - (B \cup C)$.
   (e) $A - (B \cup C) = (A - B) \cap (A - C)$.

2. The **symmetric difference** $A \Delta B$ of two sets A and B is defined by

$$A \Delta B = (A - B) \cup (B - A).$$

   Show that
   (a) $A \Delta B = (A \cup B) - (A \cap B) = B \Delta A$.
   (b) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.
   (c) $A \cup B = (A \Delta B) \Delta (A \cap B)$.
   (d) $A - B = A \Delta (A \cap B)$.

3. Let $\mathcal{R}$ be a nonempty collection of sets with the property that $A, B \in \mathcal{R}$ implies that both $A \cap B$ and $A \Delta B$ are also in $\mathcal{R}$. Show that $\mathcal{R}$ must contain the empty set, $A \cup B$ and $A - B$. (The collection $\mathcal{R}$ is called a **ring of sets**, and is of fundamental importance in measure theory and Lebesgue integration.)

0.2 MAPPINGS

Given two sets S and T, a **mapping** or **function** f from S to T is a rule which assigns a *unique* element $y \in T$ to each element $x \in S$. Symbolically, we write this mapping as $f: S \rightarrow T$ or $f: x \mapsto f(x)$ (this use of the colon should not be confused with its usage meaning “such that”). The set S is called the **domain** of f and T is called the **range** of f. Each point $f(x) \in T$ is called the **image** of x under f (or the **value** of f at x), and the collection $\{f(x) \in T: x \in S\}$ of all such image points is called the **image** of f. In general, whenever a new mapping is given, we must check to see that it is in fact **well-defined**. In other words, we must verify that $x = y$ implies $f(x) = f(y)$. We will use this requirement several times throughout the text.

If $A \subset S$, the set $\{f(x): x \in A\}$ is called the **image** of A under f and is denoted by $f(A)$. If f is a mapping from S to T and $A \subset S$, then the **restriction** of f to A, denoted by $f|A$ (or sometimes f_A), is the function from A to T defined by $f|A: x \in A \mapsto f(x) \in T$. If $x' \in T$, then any element $x \in S$ such that $f(x) = x'$ is called an **inverse image** of x' (this is sometimes also called a **preimage** of x'). Note that in general there may be more than one inverse image for any particular $x' \in T$. Similarly, if $A' \subset T$, then the inverse image of A' is the subset of S given by $\{x \in S: f(x) \in A'\}$. We will denote the inverse image of A' by $f^{-1}(A')$.

Let f be a mapping from S to T. Note that every element of T need not necessarily be the image of some element of S. However, if $f(S) = T$, then f is said to be **onto** or **surjective**. In other words, f is surjective if given any $x' \in T$ there exists $x \in S$ such that $f(x) = x'$. In addition, f is said to be **one-to-one** or **injective** if $x \neq y$ implies that $f(x) \neq f(y)$. An alternative characterization is to say that f is injective if $f(x) = f(y)$ implies that $x = y$.

If f is both injective and surjective, then f is said to be **bijective**. In this case, given any $x' \in T$ there exists a *unique* $x \in S$ such that $x' = f(x)$. If f is bijective, then we may define the **inverse mapping** $f^{-1}: T \to S$ in the following way. For any $x' \in T$, we let $f^{-1}(x')$ be that (unique) element $x \in S$ such that $f(x) = x'$.

Example 0.3 Consider the function $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$. This mapping is clearly not surjective since $f(x) \geq 0$ for any $x \in \mathbb{R}$. Furthermore, it is also not injective. Indeed, it is clear that $2 \neq -2$ but $f(2) = f(-2) = 4$. Note also that both the domain and range of f are the whole set $\mathbb{R}$, but that the image of f is just the subset of all nonnegative real numbers (i.e., the set of all $x \in \mathbb{R}$ with $x \geq 0$).

On the other hand, it is easy to see that the mapping $g: \mathbb{R} \to \mathbb{R}$ defined by $g(x) = ax + b$ for any $a, b \in \mathbb{R}$ (with $a \neq 0$) is a bijection. In this case the inverse mapping is simply given by $g^{-1}(x') = (x' - b)/a$. ∫∫

Example 0.4 If f is a mapping defined on the collections $\{A_i\}$ and $\{B_i\}$ of sets, then we claim that

$$f(\cup A_i) = \cup f(A_i)$$

and

$$f^{-1}(\cup B_i) = \cup f^{-1}(B_i) \ .$$

To prove these relationships we proceed in our usual manner. Thus we have $x' \in f(\cup A_i)$ if and only if $x' = f(x)$ for some $x \in \cup A_i$, hence if and only if x' is in some $f(A_i)$, and therefore if and only if $x' \in \cup f(A_i)$. This proves the first statement. As to the second statement, we have $x \in f^{-1}(\cup B_i)$ if and only if $f(x) \in \cup B_i$, hence if and only if $f(x)$ is in some B_i, hence if and only if x is in some $f^{-1}(B_i)$, and therefore if and only if $x \in \cup f^{-1}(B_i)$.

Several similar relationships that will be referred to again are given in the exercises. ∫∫

Now consider the sets S, T and U along with the mappings f: S → T and g: T → U. We define the **composite mapping** (sometimes also called the **product**) $g \circ f: S \to U$ by

$$(g \circ f)(x) = g(f(x))$$

for all $x \in S$. In general, $f \circ g \neq g \circ f$, and we say that the composition of two functions is not **commutative**. However, if we also have a mapping h: U → V, then for any $x \in S$ we have

$$\begin{aligned}(h \circ (g \circ f))(x) &= h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x))\\ &= ((h \circ g) \circ f)(x)\end{aligned}$$

This means that

$$h \circ (g \circ f) = (h \circ g) \circ f$$

and hence the composition of mappings is **associative**.

As a particular case of the composition of mappings, note that if f: S → T is a bijection and $f(x) = x' \in T$ where $x \in S$, then

$$(f \circ f^{-1})(x') = f(f^{-1}(x')) = f(x) = x'$$

and

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(x') = x \ .$$

If we write $f \circ f^{-1} = I_T$, then the mapping I_T has the property that $I_T(x') = x'$ for every $x' \in T$. We call I_T the **identity mapping** on T. Similarly, the composition mapping $f^{-1} \circ f = I_S$ is called the identity mapping on S. In the particular case that S = T, then $f \circ f^{-1} = f^{-1} \circ f = I$ is also called the identity mapping.

An extremely important result follows by noting that (even if $S \neq T$)

$$\begin{aligned}(f^{-1} \circ g^{-1})(g \circ f)(x) &= (f^{-1} \circ g^{-1})(g(f(x))) = f^{-1}(g^{-1}(g(f(x))))\\ &= f^{-1}(f(x)) = x\end{aligned}$$

Since it is also easy to see that $(g \circ f)(f^{-1} \circ g^{-1})(x') = x'$, we have shown that

$$(g \circ f\,)^{-1} = f^{-1} \circ g^{-1} \ .$$

Exercises

1. Let f be a mapping of sets. For each of the following, state any conditions on f that may be required (e.g., surjective or injective), and then prove the statement:
   (a) $A_1 \subset A_2$ implies $f(A_1) \subset f(A_2)$.
   (b) $f(A)^c \subset f(A^c)$ is true if and only if f is surjective.
   (c) $f(\cap A_i) \subset \cap f(A_i)$.
   (d) $B_1 \subset B_2$ implies $f^{-1}(B_1) \subset f^{-1}(B_2)$.
   (e) $f^{-1}(\cap B_i) = \cap f^{-1}(B_i)$.
   (f) $f^{-1}(B^c) = f^{-1}(B)^c$.

2. Given a nonempty set A, we define the **identity mapping** $i_A\colon A \to A$ by $i_A(a) = a$ for every $a \in A$. Let $f\colon A \to A$ be any mapping.
   (a) Show that $f \circ i_A = i_A \circ f = f$.
   (b) If f is bijective (so that f^{-1} exists), show that $f \circ f^{-1} = f^{-1} \circ f = i_A$.
   (c) Let f be a bijection, and suppose that g is any other mapping with the property that $g \circ f = f \circ g = i_A$. Show that $g = f^{-1}$.

0.3 ORDERINGS AND EQUIVALENCE RELATIONS

Given any two sets S and T, a subset R of S × T is said to be a **relation** between S and T. If $R \subset S \times T$ and $(x, y) \in R$, then it is common to write xRy to show that x and y are "R-related." In particular, consider the relation symbolized by ≤ and defined as having the following properties on a set S:

(a) $x \le x$ (reflexivity);
(b) $x \le y$ and $y \le x$ implies $x = y$ for all $x, y \in S$ (antisymmetry);
(c) $x \le y$ and $y \le z$ implies $x \le z$ for all $x, y, z \in S$ (transitivity).

Any relation on a non-empty set S having these three properties is said to be a **partial ordering**, and S is said to be a **partially ordered set**. We will sometimes write $y \ge x$ instead of the equivalent notation $x \le y$. The reason for including the qualifying term "partial" in this definition is shown in our next example.

Example 0.5 Let S be any set, and let $\mathcal{P}(S)$ be the collection of all subsets of S (this is sometimes called the **power set** of S). If A, B and C are subsets of S, then clearly $A \subset A$ so that (a) is satisfied; $A \subset B$ and $B \subset A$ implies $A = B$ then satisfies (b); and $A \subset B$ and $B \subset C$ implies $A \subset C$ satisfies (c). Therefore

$\subset$ defines a partial ordering on $\mathcal{P}(S)$, and the subsets of S are said to be **ordered by inclusion**. Note however, that if $A \subset S$ and $B \subset S$ but $A \not\subset B$ and $B \not\subset A$, then there is no relation between A and B, and we say that A and B are not **comparable**. ∕∕

The terminology used in this example is easily generalized as follows. If S is any partially ordered set and $x, y \in S$, then we say that x and y are **comparable** if either $x \le y$ or $y \le x$.

If, in addition to properties (a) – (c), a relation R also has the property that any two elements are comparable, then R is said to be a **total ordering**. In other words, a total ordering also has the property that

(d) either $x \le y$ or $y \le x$ for all $x, y \in S$.

Let S be a set partially ordered by $\le$ and suppose $A \subset S$. It should be clear that A may be considered to be a partially ordered set by defining $a \le b$ for all $a, b \in A$ if $a \le b$ where a and b are considered to be elements of S. (This is similar to the restriction of a mapping.) We then say that A has a partial ordering $\le$ **induced** by the ordering on S. If A is *totally* ordered by the ordering induced by $\le$, then A is frequently called a **chain** in S.

Let A be a non-empty subset of a partially ordered set S. An element $x \in S$ is called an **upper bound** for A if $a \le x$ *for all* $a \in A$. If it so happens that x is an element of A, then x is said to be a **largest element** of A. Similarly, $y \in S$ is called a **lower bound** for A if $y \le a$ *for all* $a \in A$, and y is a **smallest element** of A if $y \in A$. If A has an upper (lower) bound, then we say that A is **bounded above** (**below**). Note that largest and smallest elements need not be unique.

Suppose that A is bounded above by $\alpha \in S$, and in addition, suppose that for any other upper bound x of A we have $\alpha \le x$. Then we say that α is a **least upper bound** (or **supremum**) of A, and we write $\alpha = \text{lub } A = \sup A$. As expected, if A is bounded below by $\beta \in S$, and if $y \le \beta$ for all other lower bounds $y \in S$, then β is called a **greatest lower bound** (or **infimum**), and we write $\beta = \text{glb } A = \inf A$. In other words, if it exists, the least upper (greatest lower) bound for A is a smallest (largest) element of the set of all upper (lower) bounds for A.

From property (b) above and the definitions of inf and sup, we see that if they exist, the least upper bound and the greatest lower bound are unique. (For example, if β and β' are both greatest lower bounds, then $\beta \le \beta'$ and $\beta' \le \beta$ implies that $\beta = \beta'$.) Hence it is meaningful to talk about *the* least upper bound and *the* greatest lower bound.

Let S be a partially ordered set, and suppose $A \subset S$. An element $\alpha \in A$ is said to be **maximal in A** if for any element $a \in A$ with $\alpha \le a$, we have $a = \alpha$. In other words, no element of A other than α itself is greater than or equal to

α. Similarly, an element $\beta \in A$ is said to be **minimal in A** if for any $b \in A$ with $b \leq \beta$, we have $b = \beta$. Note that a maximal element may not be a largest element (since two elements of a partially ordered set need not be comparable), and there may be many maximal elements in A.

We now state Zorn's lemma, one of the most fundamental results in set theory, and hence in all of mathematics. While the reader can hardly be expected to appreciate the significance of this lemma at the present time, it is in fact extremely powerful.

Zorn's Lemma Let S be a partially ordered set in which every chain has an upper bound. Then S contains a maximal element.

It can be shown (see any book on set theory) that Zorn's lemma is logically equivalent to the **axiom of choice**, which states that given any non-empty family of non-empty disjoint sets, a set can be formed which contains precisely one element taken from each set in the family. Although this seems like a rather obvious statement, it is important to realize that either the axiom of choice or some other statement equivalent to it must be postulated in the formulation of the theory of sets, and thus Zorn's lemma is not really provable in the usual sense. In other words, Zorn's lemma is frequently taken as an axiom of set theory. However, it is an indispensable part of some of what follows although we shall have little occasion to refer to it directly.

Up to this point, we have only talked about one type of relation, the partial ordering. We now consider another equally important relation. Let S be any set. A relation $\approx$ on S is said to be an **equivalence relation** if it has the following properties for all $x, y, z \in S$:

(a) $x \approx x$ for all $x \in S$ (reflexivity);
(b) $x \approx y$ implies $y \approx x$ (symmetry);
(c) $x \approx y$ and $y \approx z$ implies $x \approx z$ for all $x, y, z \in S$ (transitivity).

Note that only (b) differs from the defining relations for a partial ordering.

A **partition** of a set S is a family $\{S_i\}$ of non-empty subsets of S such that $\cup S_i = S$ and $S_i \cap S_j \neq \varnothing$ implies $S_i = S_j$. Suppose $x \in S$ and let $\approx$ be an equivalence relation on S. The subset of S defined by $[x] = \{y: y \approx x\}$ is called the **equivalence class** of x. The most important property of equivalence relations is contained in the following theorem.

Theorem 0.2 The family of all distinct equivalence classes of a set S forms a partition of S. (This is called the partition induced by $\approx$.) Moreover, given any partition of S, there is an equivalence relation on S that induces this partition.

Proof Let $\approx$ be an equivalence relation on a set S, and let x be any element of S. Since $x \approx x$, it is obvious that $x \in [x]$. Thus each element of S lies in at least one non-empty equivalence class. We now show that any two equiv–alence classes are either disjoint or are identical. Let $[x_1]$ and $[x_2]$ be two equivalence classes, and let y be a member of both classes. In other words, $y \approx x_1$ and $y \approx x_2$. Now choose any $z \in [x_1]$ so that $z \approx x_1$. But this means that $z \approx x_1 \approx y \approx x_2$ so that any element of $[x_1]$ is also an element of $[x_2]$, and hence $[x_1] \subset [x_2]$. Had we chosen $z \in [x_2]$ we would have found that $[x_2] \subset [x_1]$. Therefore $[x_1] = [x_2]$, and we have shown that if two equivalence classes have any element in common, then they must in fact be identical.

Let $\{S_i\}$ be any partition of S. We define an equivalence relation on S by letting $x \approx y$ if $x, y \in S_i$ for any $x, y \in S$. It should be clear that this does indeed satisfy the three conditions for an equivalence relation, and that this equivalence relation induces the partition $\{S_i\}$. ∎

As we will see in the next chapter, this theorem has a direct analogue in the theory of groups.

Exercises

1. Let $\mathbb{Z}^+$ denote the set of positive integers. We write $m|n$ to denote the fact that m divides n, i.e., $n = km$ for some $k \in \mathbb{Z}^+$.

(a) Show that $|$ defines a partial ordering on $\mathbb{Z}^+$.

(b) Does $\mathbb{Z}^+$ contain either a maximal or minimal element relative to this partial ordering?

(c) Prove that any subset of $\mathbb{Z}^+$ containing exactly two elements has a greatest lower bound and a least upper bound.

(d) For each of the following subsets of $\mathbb{Z}^+$, determine whether or not it is a chain in $\mathbb{Z}^+$, find a maximal and minimal element, an upper and lower bound, and a least upper bound:

(i) $\{1, 2, 4, 6, 8\}$.
(ii) $\{1, 2, 3, 4, 5\}$.
(iii) $\{3, 6, 9, 12, 15, 18\}$.
(iv) $\{4, 8, 16, 32, 64, 128\}$.

2. Define a relation ≈ on ℝ by requiring that $a \approx b$ if $|a| = |b|$. Show that this defines an equivalence relation on ℝ.

3. For any $a, b \in \mathbb{R}$, let $a \sim b$ mean $ab > 0$. Does ~ define an equivalence relation? What happens if we use $ab \geq 0$ instead of $ab > 0$?

0.4 CARDINALITY AND THE REAL NUMBER SYSTEM

We all have an intuitive sense of what it means to say that two finite sets have the same number of elements, but our intuition leads us astray when we come to consider infinite sets. For example, there are as many perfect squares (1, 4, 9, 16, etc.) among the positive integers as there are positive integers. That this is true can easily be seen by writing each positive integer paired with its square:

$$\begin{array}{ccccc} 1, & 2, & 3, & 4, & \dots \\ 1^2, & 2^2, & 3^2, & 4^2, & \dots \end{array}$$

While it seems that the perfect squares are only sparsely placed throughout the integers, we have in fact constructed a bijection of all positive integers with all of the perfect squares of integers, and we are forced to conclude that in this sense they both have the "same number of elements."

In general, two sets S and T are said to have the same **cardinality**, or to possess the same number of elements, if there exists a bijection from S to T. A set S is **finite** if it has the same cardinality as either ∅ or the set $\{1, 2, \dots, n\}$ for some positive integer n; otherwise, S is said to be **infinite**. However, there are varying degrees of "infinity." A set S is **countable** if it has the same cardinality as a subset of the set $\mathbb{Z}^+$ of positive integers. If this is not the case, then we say that S is **uncountable**. Any infinite set which is numerically equivalent to (i.e., has the same cardinality as) $\mathbb{Z}^+$ is said to be **countably infinite**. We therefore say that a set is **countable** if it is countably infinite or if it is non-empty and finite.

It is somewhat surprising (as was first discovered by Cantor) that the set $\mathbb{Q}^+$ of all positive rational numbers is in fact countable. The elements of $\mathbb{Q}^+$ can not be listed in order of increasing size because there is no smallest such number, and between any two rational numbers there are infinitely many others (see Theorem 0.4 below). To show that $\mathbb{Q}^+$ is countable, we shall construct a bijection from $\mathbb{Z}^+$ to $\mathbb{Q}^+$.

To do this, we first consider all positive rationals whose numerator and denominator add up to 2. In this case we have only $1/1 = 1$. Next we list those positive rationals whose numerator and denominator add up to 3. If we agree to always list our rationals with numerators in increasing order, then we have 1/2 and 2/1 = 2. Those rationals whose numerator and denominator add up to 4 are then given by 1/3, 2/2 = 1, 3/1 = 3. Going on to 5 we obtain 1/4, 2/3, 3/2, 4/1 = 4. For 6 we have 1/5, 2/4 = 1/2, 3/3 = 1, 4/2 = 2, 5/1 = 5. Continuing with this procedure, we list together all of our rationals, omitting any number already listed. This gives us the sequence

$$1, 1/2, 2, 1/3, 3, 1/4, 2/3, 3/2, 4, 1/5, 5, \dots$$

which contains each positive rational number exactly once, and provides our desired bijection.

We have constructed several countably infinite sets of real numbers, and it is natural to wonder whether there are in fact any uncountably infinite sets. It was another of Cantor's discoveries that the set $\mathbb{R}$ of all real numbers is actually uncountable. To prove this, let us assume that we have listed (in some manner similar to that used for the set $\mathbb{Q}^+$) all the real numbers in decimal form. What we shall do is construct a decimal $.d_1d_2d_3\cdots$ that is not on our list, thus showing that the list can not be complete. Consider only the portion of the numbers on our list to the right of the decimal point, and look at the first number on the list. If the first digit after the decimal point of the first number is a 1, we let $d_1 = 2$; otherwise we let $d_1 = 1$. No matter how we choose the remaining d's, our number will be different from the first on our list. Now look at the second digit after the decimal point of the second number on our list. Again, if this second digit is a 1, we let $d_2 = 2$; otherwise we let $d_2 = 1$. We have now constructed a number that differs from the first two numbers on our list. Continuing in this manner, we construct a decimal $.d_1d_2d_3\cdots$ that differs from every other number on our list, contradicting the assumption that all real numbers can be listed, and proving that $\mathbb{R}$ is actually uncountable.

Since it follows from what we showed above that the set $\mathbb{Q}$ of all rational numbers on the real line is countable, and since we just proved that the set $\mathbb{R}$ is uncountable, it follows that a set of **irrational** numbers must exist and be uncountably infinite.

From now on we will assume that the reader understands what is meant by the real number system, and we proceed to investigate some of its most useful properties. A complete axiomatic treatment that justifies what we already know would take us too far afield, and the interested reader is referred to, e.g., Rudin (1976).

Let S be any ordered set, and let $A \subset S$ be non-empty and bounded above. We say that S has the **least upper bound property** if sup A exists in S. In the special case of $S = \mathbb{R}$, we have the following extremely important axiom.

Archimedean Axiom Every non-empty set of real numbers which has an upper (lower) bound has a least upper bound (greatest lower bound).

The usefulness of this axiom is demonstrated in the next rather obvious though important result, sometimes called the **Archimedean property** of the real number line.

Theorem 0.3 Let a, $b \in \mathbb{R}$ and suppose $a > 0$. Then there exists $n \in \mathbb{Z}^+$ such that $na > b$.

Proof Let S be the set of all real numbers of the form na where n is a positive integer. If the theorem were false, then b would be an upper bound for S. But by the Archimedean axiom, S has a least upper bound $\alpha = \sup S$. Since $a > 0$, we have $\alpha - a < \alpha$ and $\alpha - a$ can not be an upper bound of S (by definition of α). Therefore, there exists an $m \in \mathbb{Z}^+$ such that $ma \in S$ and $\alpha - a < ma$. But then $\alpha < (m + 1)a \in S$ which contradicts the fact that $\alpha = \sup S$. ∎

One of the most useful facts about the real line is that the set $\mathbb{Q}$ of all rational numbers is **dense** in $\mathbb{R}$. By this we mean that given any two distinct real numbers, we can always find a rational number between them. This means that any real number may be approximated to an arbitrary degree of accuracy by a rational number. It is worth proving this using Theorem 0.3.

Theorem 0.4 Suppose x, $y \in \mathbb{R}$ and assume that $x < y$. Then there exists a rational number $p \in \mathbb{Q}$ such that $x < p < y$.

Proof Since $x < y$ we have $y - x > 0$. In Theorem 0.3, choose $a = y - x$ and $b = 1$ so there exists $n \in \mathbb{Z}^+$ such that $n(y - x) > 1$, or alternatively,

$$1 + nx < ny \ .$$

Applying Theorem 0.3 again, we let $a = 1$ and both $b = nx$ and $b = -nx$ to find integers $m_1, m_2 \in \mathbb{Z}^+$ such that $m_1 > nx$ and $m_2 > -nx$. Rewriting the second of these as $-m_2 < nx$, we combine the two inequalities to obtain

$$-m_2 < nx < m_1$$

so that nx lies between two integers. But if nx lies between two integers, it must lie between two consecutive integers $m - 1$ and m for some $m \in \mathbb{Z}$ where $-m_2 \le m \le m_1$. Thus $m - 1 \le nx < m$ implies that $m \le 1 + nx$ and $nx < m$. We therefore obtain

$$nx < m \le 1 + nx < ny$$

or, equivalently (since $n \neq 0$), $x < m/n < y$. ∎

Corollary Suppose $x, y \in \mathbb{R}$ and assume that $x < y$. Then there exist integers $m \in \mathbb{Z}$ and $k \ge 0$ such that $x < m/2^k < y$.

Proof Simply note that the proof of Theorem 0.4 could be carried through if we choose an integer $k \ge 0$ so that $2^k(y - x) > 1$, and replace n by 2^k throughout. ∎

In addition to the real number system $\mathbb{R}$ we have been discussing, it is convenient to introduce the **extended real number system** as follows. To the real number system $\mathbb{R}$, we adjoin the symbols $+\infty$ and $-\infty$ which are *defined* to have the property that $-\infty < x < +\infty$ *for all* $x \in \mathbb{R}$. This is of great notational convenience. We stress however, that neither $+\infty$ or $-\infty$ are considered to be elements of $\mathbb{R}$.

Suppose A is a non-empty set of real numbers. We have already defined sup A in the case where A has an upper bound. If A is non-empty and has no upper bound, then we say that $\sup A = +\infty$, and if $A = \varnothing$, then $\sup A = -\infty$. Similarly, if $A \neq \varnothing$ and has no lower bound, then $\inf A = -\infty$, and if $A = \varnothing$, then $\inf A = +\infty$.

Suppose $a, b \in \mathbb{R}$ with $a \le b$. Then the **closed interval** [a, b] from a to b is the subset of $\mathbb{R}$ defined by

$$[a, b] = \{x \in \mathbb{R}: a \le x \le b\} .$$

Similarly, the **open interval** (a, b) is defined to be the subset

$$(a, b) = \{x \in \mathbb{R}: a < x < b\} .$$

We may also define the **open-closed** and **closed-open** intervals in the obvious way. The **infinity symbols** $\pm\infty$ thus allow us to talk about intervals of the form $(-\infty, b]$, $[a, +\infty)$ and $(-\infty, +\infty)$.

Another property of the sup that will be needed later on is contained in the following theorem. By way of notation, we define $\mathbb{R}^+$ to be the set of all real numbers > 0, and $\bar{\mathbb{R}}^+ = \mathbb{R}^+ \cup \{0\}$ to be the set of all real numbers ≥ 0.

Theorem 0.5 Let A and B be non-empty bounded sets of real numbers, and define the sets

$$A + B = \{x + y: x \in A \text{ and } y \in B\}$$

and

$$AB = \{xy: x \in A \text{ and } y \in B\} .$$

Then

(a) For all $A, B \subset \mathbb{R}$ we have $\sup(A + B) = \sup A + \sup B$.

(b) For all $A, B \subset \bar{\mathbb{R}}^+$ we have $\sup(AB) \le (\sup A)(\sup B)$.

Proof (a) Let $\alpha = \sup A$, $\beta = \sup B$, and suppose $x + y \in A + B$. Then

$$x + y \le \alpha + y \le \alpha + \beta$$

so that $\alpha + \beta$ is an upper bound for $A + B$. Now note that given $\varepsilon > 0$, there exists $x \in A$ such that $\alpha - \varepsilon/2 < x$ (or else α would not be the least upper bound). Similarly, there exists $y \in B$ such that $\beta - \varepsilon/2 < y$. Then $\alpha + \beta - \varepsilon < x + y$ so that $\alpha + \beta$ must be the least upper bound for $A + B$.

(b) If $x \in A \subset \bar{\mathbb{R}}^+$ we must have $x \le \sup A$, and if $y \in B \subset \bar{\mathbb{R}}^+$ we have $y \le \sup B$. Hence $xy \le (\sup A)(\sup B)$ for all $xy \in AB$, and therefore $A \ne \varnothing$ and $B \ne \varnothing$ implies

$$\sup(AB) \le (\sup A)(\sup B) .$$

The reader should verify that strict equality holds if $A \subset \mathbb{R}^+$ and $B \subset \mathbb{R}^+$. ∎

The last topic in our treatment of real numbers that we wish to discuss is the absolute value. Note that if $x \in \mathbb{R}$ and $x^2 = a$, then we also have $(-x)^2 = a$. We *define* $\sqrt{a}$, for $a \ge 0$, to be the unique *positive* number x such that $x^2 = a$, and we call x the **square root** of a.

Suppose $x, y \ge 0$ and let $x^2 = a$ and $y^2 = b$. Then $x = \sqrt{a}$, $y = \sqrt{b}$ and we have $(\sqrt{a}\sqrt{b})^2 = (xy)^2 = x^2 y^2 = ab$ which implies that

$$\sqrt{ab} = \sqrt{a}\sqrt{b} .$$

For any $a \in \mathbb{R}$, we define its **absolute value** $|a|$ by $|a| = \sqrt{a^2}$. It then follows that $|-a| = |a|$, and hence

$$|a| = \begin{cases} a \text{ if } a \ge 0 \\ -a \text{ if } a < 0 \end{cases}$$

This clearly implies that

$$a \le |a| .$$

In addition, if $a, b \ge 0$ and $a \le b$, then we have $(\sqrt{a})^2 = a \le b = (\sqrt{b})^2$ so that $\sqrt{a} \le \sqrt{b}$.

The absolute value has two other useful properties. First, we note that

$$|ab| = \sqrt{(ab)^2} = \sqrt{a^2b^2} = \sqrt{a^2}\sqrt{b^2} = |a||b|.$$

Second, we see that

$$\begin{aligned}|a+b|^2 &= (a+b)^2\\ &= a^2+b^2+2ab\\ &\le |a|^2+|b|^2+2|ab|\\ &= |a|^2+|b|^2+2|a||b|\\ &= (|a|+|b|)^2\end{aligned}$$

and therefore

$$|a + b| \le |a| + |b| \;.$$

Using these results, many other useful relationships may be obtained. For example, $|a| = |a + b - b| \le |a + b| + |-b| = |a + b| + |b|$ so that

$$|a| - |b| \le |a + b| \;.$$

Others are to be found in the exercises.

Example 0.6 Let us show that if $\varepsilon > 0$, then $|x| < \varepsilon$ if and only if $-\varepsilon < x < \varepsilon$. Indeed, we see that if $x > 0$, then $|x| = x < \varepsilon$, and if $x < 0$, then $|x| = -x < \varepsilon$ which implies $-\varepsilon < x < 0$ (we again use the fact that $a < b$ implies $-b < -a$). Combining these results shows that $|x| < \varepsilon$ implies $-\varepsilon < x < \varepsilon$. We leave it to the reader to reverse the argument and complete the proof.

A particular case of this result that will be of use later on comes from letting $x = a - b$. We then see that $|a - b| < \varepsilon$ if and only if $-\varepsilon < a - b < \varepsilon$. Rearranging, this may be written in the form $b - \varepsilon < a < b + \varepsilon$. The reader should draw a picture of this relationship. ∕∕

Exercises

1. Prove that if A and B are countable sets, then A × B is countable.

2. (a) A real number x is said to be **algebraic** (over the rationals) if it satisfies some polynomial equation of positive degree with rational coefficients:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \ .$$

Given the fact (which we will prove in Chapter 6) that each polynomial equation has only finitely many roots, show that the set of all algebraic numbers is countable.

(b) We say that a real number x is **transcendental** if it is not algebraic (the most common transcendental numbers are π and e). Using the fact that the reals are uncountable, show that the set of all transcendental numbers is also uncountable.

3. If $a, b \geq 0$, show that $\sqrt{ab} \leq (a + b)/2$.

4. For any $a, b \in \mathbb{R}$, show that:
   (a) $|\,|a| - |b|\,| \leq |a + b|$.
   (b) $|\,|a| - |b|\,| \leq |a - b|$.

5. (a) If $A \subset \mathbb{R}$ is nonempty and bounded below, show $\sup(-A) = -\inf A$.
   (b) If $A \subset \mathbb{R}$ is nonempty and bounded above, show $\inf(-A) = -\sup A$.

0.5 INDUCTION

Another important concept in the theory of sets is called “well-ordering.” In particular, we say that a totally ordered set S is **well-ordered** if *every* nonempty subset A of S has a smallest element. For example, consider the set S of all rational numbers in the interval [0, 1]. It is clear that 0 is the smallest element of S, but the subset of S consisting of all rational numbers > 0 has no smallest element (this is a consequence of Theorem 0.4).

For our purposes, it is an (apparently obvious) axiom that every nonempty set of natural numbers has a smallest element. In other words, the natural numbers are well-ordered. The usefulness of this axiom is that it allows us to prove an important property called **induction**.

Theorem 0.6 Assume that for all $n \in \mathbb{Z}^+$ we are given an assertion A(n), and assume it can be shown that:

(a) A(1) is true;
(b) If A(n) is true, then A(n + 1) is true.

Then A(n) is true for all $n \in \mathbb{Z}^+$.

Proof If we let S be that subset of $\mathbb{Z}^+$ for which A(n) is not true, then we must show that $S = \varnothing$. According to our well-ordering axiom, if $S \neq \varnothing$ then S contains a least element which we denote by N. By assumption (a), we must have N ≠ 1 and hence N > 1. Since N is a least element, N − 1 ∉ S so that A(N − 1) must be true. But then (b) implies that A(N) must be true which contradicts the definition of N. ∎

Example 0.7 Let n > 0 be an integer. We define **n factorial**, written n!, to be the number

$$n! = n(n-1)(n-2)\cdots(2)(1)$$

with 0! defined to be 1. The **binomial coefficient** $\binom{n}{k}$ is defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

where n and k are nonnegative integers. We leave it to the reader (see Exercise 0.6.1) to show that

$$\binom{n}{k} = \binom{n}{n-k}$$

and

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

What we wish to prove is the **binomial theorem**:

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} \quad .$$

We proceed by induction as follows. For n = 1, we have

$$\binom{1}{0}x^0y^1 + \binom{1}{1}x^1y^0 = (x+y)^1$$

so that the assertion is true for n = 1. We now assume the theorem holds for n, and proceed to show that it also holds for n + 1. We have

$$\begin{aligned}(x+y)^{n+1} &= (x+y)(x+y)^n = (x+y)\left[\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\right] \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k+1}\end{aligned} \qquad (*)$$

By relabelling the summation index, we see that for any function f with domain equal to {0, 1, . . . , n} we have

$$\sum_{k=0}^{n} f(k) = f(0) + f(1) + \cdots + f(n) = \sum_{k=1}^{n+1} f(k-1).$$

We use this fact in the first sum in (*), and separate out the k = 0 term in the second to obtain

$$(x+y)^{n+1} = \sum_{k=1}^{n+1} \binom{n}{k-1} x^k y^{n-k+1} + y^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^{k+1} y^{n-k+1}.$$

We now separate out the k = n + 1 term from the first sum in this expression and group terms to find

$$\begin{aligned}(x+y)^{n+1} &= x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k} \right] x^k y^{n-k+1} \\ &= x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n+1-k} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}\end{aligned}$$

as was to be shown. ∕∕

0.6 COMPLEX NUMBERS

At this time we wish to formally define the complex number system $\mathbb{C}$, although most readers should already be familiar with its basic properties. The motivation for the introduction of such numbers comes from the desire to solve equations such as $x^2 + 1 = 0$ which leads to the square root of a negative number. We may proceed by manipulating square roots of negative numbers as if they were square roots of positive numbers. However, a consequence of this is that on the one hand, $(\sqrt{-1}\,)^2 = -1$, while on the other hand

$$(\sqrt{-1}\,)^2 = \sqrt{-1}\sqrt{-1} = \sqrt{(-1)(-1)} = \sqrt{+1} = 1 .$$

In order to avoid paradoxical manipulations of this type, the symbol i was introduced by Euler (in 1779) with the defining property that $i^2 = -1$. Then, if $a > 0$, we have $\sqrt{-a} = i\sqrt{a}$. Using this notation, a **complex number** $z \in \mathbb{C}$ is a number of the form z = x+ *i*y where x ∈ ℝ is called the **real part** of z (written Re z), and y ∈ ℝ is called the **imaginary part** of z (written Im z).

Two complex numbers x + *i*y and u + *i*v are said to be equal if x = u and y = v. Algebraic operations in ℂ are *defined* as follows:

Addition: $(x + iy) + (u + iv) = (x + u) + i(y + v)$.
Subtraction: $(x + iy) - (u + iv) = (x - u) + i(y - v)$.
Multiplication: $(x + iy)(u + iv) = (xu - yv) + i(xv + yu)$.
Division: $(x + iy)/(u + iv) = (x + iy)(u - iv)/(u + iv)(u - iv)$
$= [(xu + yv) + i(yu - vx)]/(u^2 + v^2)$.

It should be clear that the results for multiplication and division may be obtained by formally multiplying out the terms and using the fact that $i^2 = -1$.

The **complex conjugate** z* of a complex number z = x + *i*y is defined to be the complex number z* = x − *i*y. Note that if z, w ∈ ℂ we have

$$\begin{aligned}(z+w)^* &= z^* + w^*\\ (zw)^* &= z^* w^*\\ z + z^* &= 2\operatorname{Re} z\\ z - z^* &= 2i\operatorname{Im} z\end{aligned}$$

The **absolute value** (or **modulus**) |z| of a complex number z = x + *i*y is defined to be the real number

$$|z| = \sqrt{x^2 + y^2} = (zz^*)^{1/2}\,.$$

By analogy to the similar result for real numbers, if z, w ∈ ℂ then (using the fact that z = x + *i*y implies $\operatorname{Re} z = x \le \sqrt{x^2+y^2} = |z|$)

$$\begin{aligned}|z+w|^2 &= (z+w)(z+w)^*\\ &= zz^* + zw^* + z^*w + ww^*\\ &= |z|^2 + 2\operatorname{Re}(zw^*) + |w|^2\\ &\le |z|^2 + 2|zw^*| + |w|^2\\ &= |z|^2 + 2|z||w| + |w|^2\\ &= (|z| + |w|)^2\end{aligned}$$

and hence taking the square root of both sides yields

$$|z + w| \le |z| + |w|\ .$$

Let the sum $z_1 + \cdots + z_n$ be denoted by $\sum_{i=1}^{n} z_i$. The following theorem is known as **Schwartz's inequality**.

Theorem 0.7 Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be complex numbers. Then

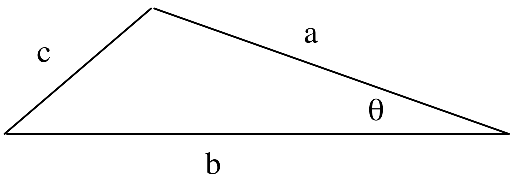
$$\left|\sum_{j=1}^{n} a_j b_j{}^*\right| \le \left(\sum_{j=1}^{n} |a_j|^2\right)\left(\sum_{j=1}^{n} |b_j|^2\right)$$

Proof Write (suppressing the limits on the sum) $A = \sum_j |a_j|^2$, $B = \sum_j |b_j|^2$ and $C = \sum_j a_j b_j{}^*$. If $B = 0$, then $b_j = 0$ for all $j = 1, \ldots, n$ and there is nothing to prove, so we assume that $B \neq 0$. We then have

$$\begin{aligned}
0 &\le \textstyle\sum_i |Ba_i - Cb_i|^2 \\
&= \textstyle\sum_i (Ba_i - Cb_i)(Ba_i{}^* - Cb_i{}^*) \\
&= B^2 \textstyle\sum_i |a_i|^2 - BC^* \sum_i a_i b_i{}^* - BC \sum_i a_i{}^* b_i + |C|^2 \sum_i |b_i|^2 \\
&= B^2 A - B|C|^2 - B|C|^2 + |C|^2 B \\
&= B(AB - |C|^2).
\end{aligned}$$

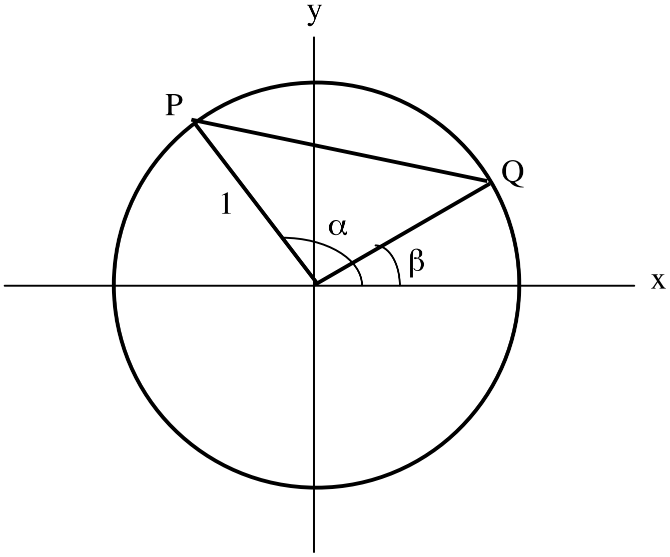
But $B \ge 0$ so that $AB - |C|^2 \ge 0$ and hence $|C|^2 \le AB$. ∎

It is worth our going through some additional elementary properties of complex numbers that will be needed on occasion throughout this text. Purely for the sake of logical consistency, let us first prove some basic trigonometric relationships. Our starting point will be the so-called "law of cosines" which states that $c^2 = a^2 + b^2 - 2ab\cos\theta$ (see the figure below).



A special case of this occurs when $\theta = \pi/2$, in which case we obtain the famous Pythagorean theorem $a^2 + b^2 = c^2$. (While most readers should already be familiar with these results, we prove them in Section 2.4.)

Now consider a triangle inscribed in a *unit* circle as shown below:



The point P has coordinates (x_P , y_P) = (cos α, sin α), and Q has coordinates (x_Q, y_Q) = (cos β, sin β). Applying the Pythagorean theorem to the right triangle with hypotenuse defined by the points P and Q (and noting $x_Q^2 + y_Q^2 = x_P^2 + y_P^2 = 1$), we see that the square of the distance between the points P and Q is given by

$$\begin{aligned}(PQ)^2 &= (x_Q - x_P)^2 + (y_Q - y_P)^2 \\ &= (x_Q{}^2 + y_Q{}^2) + (x_P{}^2 + y_P{}^2) - 2(x_P x_Q + y_P y_Q) \\ &= 2 - 2(\cos\alpha\cos\beta + \sin\alpha\sin\beta).\end{aligned}$$

On the other hand, we can apply the law of cosines to obtain the distance PQ, in which case we find that $(PQ)^2 = 2 - 2\cos(\alpha - \beta)$. Equating these expressions yields the basic result

$$\cos(\alpha - \beta) \;=\; \cos\alpha\cos\beta + \sin\alpha\sin\beta \;\; .$$

Replacing β by −β we obtain

$$\cos(\alpha + \beta) \;=\; \cos\alpha\cos\beta - \sin\alpha\sin\beta \;\; .$$

If we let α = π/2, then we have cos(π/2 − β) = sin β, and if we now replace β by π/2 − β, we find that cos β = sin(π/2 − β). Finally, we can use these last results to obtain formulas for sin(α ± β). In particular, we replace β by α + β to obtain

$$\begin{aligned}\sin(\alpha+\beta) &= \cos(\pi/2-(\alpha+\beta))\\ &= \cos(\pi/2-\alpha-\beta)\\ &= \cos(\pi/2-\alpha)\cos\beta+\sin(\pi/2-\alpha)\sin\beta\\ &= \sin\alpha\cos\beta+\cos\alpha\sin\beta\end{aligned}$$

Again, replacing β by $-\beta$ yields

$$\sin(\alpha-\beta) = \sin\alpha\cos\beta-\cos\alpha\sin\beta\ .$$

(The reader may already know that these results are simple to derive using the Euler formula $\exp(\pm i\theta) = \cos\theta \pm i\sin\theta$ which follows from the Taylor series expansions of exp x, sin x and cos x, along with the definition $i^2 = -1$.)

It is often of great use to think of a complex number $z = x + iy$ as a point in the xy-plane. If we define

$$r = |z| = \sqrt{x^2 + y^2}$$

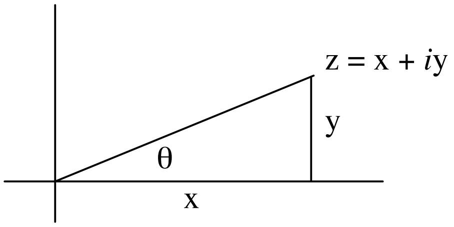
and

$$\tan\theta = y/x$$

then a complex number may also be written in the form

$$z = x + iy = r(\cos\theta + i\sin\theta) = r\exp(i\theta)$$

(see the figure below).



Given two complex numbers

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$$

and

$$z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$$

we can use the trigonometric addition formulas derived above to show that

$$z_1z_2 = r_1\,r_2[\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)]\ .$$

In fact, by induction it should be clear that this can be generalized to (see Exercise 0.6.5)

$$z_1 z_2 \cdots z_n = \\ r_1 r_2 \cdots r_n[\cos(\theta_1 + \theta_2 + \cdots + \theta_n) + i\sin(\theta_1 + \theta_2 + \cdots + \theta_n)] \ .$$

In the particular case where $z_1 = \cdots = z_n$, we find that

$$z^n = r^n(\cos n\theta + i\sin n\theta) \ .$$

This is often called **De Moivre's theorem**.

One of the main uses of this theorem is as follows. Let w be a complex number, and let $z = w^n$ (where n is a positive integer). We say that w is an n*th* **root** of z, and we write this as $w = z^{1/n}$. Next, we observe from De Moivre's theorem that writing $z = r(\cos\theta + i\sin\theta)$ and $w = s(\cos\phi + i\sin\phi)$ yields (assuming that $z \neq 0$)

$$r(\cos\theta + i\sin\theta) = s^n(\cos n\phi + i\sin n\phi) \ .$$

But $\cos\theta = \cos(\theta \pm 2k\pi)$ for $k = 0, \pm1, \pm2, \dots$, and therefore $r = s^n$ and $n\phi = \theta \pm 2k\pi$. (This follows from the fact that if $z_1 = x_1 + iy_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ and $z_2 = x_2 + iy_2 = r_2(\cos\theta_2 + i\sin\theta_2)$, then $z_1 = z_2$ implies $x_1 = x_2$ and $y_1 = y_2$ so that $r_1 = r_2$, and hence $\theta_1 = \theta_2$.) Then s is the real positive nth root of r, and $\phi = \theta/n \pm 2k\pi/n$. Since this expression for ϕ is the same if any two integers k differ by a multiple of n, we see that there are precisely n distinct solutions of $z = w^n$ (when $z \neq 0$), and these are given by

$$w = r^{1/n}[\cos(\theta + 2k\pi)/n + i\sin(\theta + 2k\pi)/n]$$

where $k = 0, 1, \dots , n - 1$.

Exercises

1. (a) Show

$$\binom{n}{k} = \binom{n}{n-k}.$$

(b) Show

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

2. Prove by induction the formula $1 + 2 + \cdots + n = n(n + 1)/2$.

3. Prove by induction the formula

$$1+x+x^2+\cdots+x^{n-1}=\frac{1-x^n}{1-x}$$

where x is any real number ≠ 1.

4. Prove by induction that for any complex numbers $z_1, \ldots, z_n$ we have:
(a)

$$\left|\sum_{i=1}^{n} z_i\right| \le \sum_{i=1}^{n}|z_i|$$

(b) $|z_1z_2 \cdots z_n| = |z_1||z_2| \cdots |z_n|$.

5. Prove by induction that for any complex numbers $z_1, \ldots, z_n$ we have

$$z_1z_2 \cdots z_n = r_1r_2 \cdots r_n[\cos(\theta_1 + \theta_2 + \cdots + \theta_n) + i \sin(\theta_1 + \theta_2 + \cdots + \theta_n)]$$

where $z_j = r_j \exp(i\theta_j)$.

0.7 ADDITIONAL PROPERTIES OF THE INTEGERS

The material of this section will be generalized in Sections 6.1 and 6.2 to the theory of polynomials. However, it will also be directly useful to us in our discussion of finite fields in Section 6.6. Most of this section should be familiar to the reader from very elementary courses.

Our first topic is the division of an arbitrary integer $a \in \mathbb{Z}$ by a positive integer $b \in \mathbb{Z}^+$. For example, we can divide 11 by 4 to obtain $11 = 2 \cdot 4 + 3$. As another example, -7 divided by 2 yields $-7 = -4 \cdot 2 + 1$. Note that each of these examples may be written in the form $a = qb + r$ where $q \in \mathbb{Z}$ and $0 \le r < b$. The number q is called the **quotient**, and the number r is called the **remainder** in the division of a by b. In the particular case that $r = 0$, we say that b **divides** a and we write this as $b|a$. If $r \neq 0$, then b does not divide a, and this is written as $b \nmid a$. If an integer $p \in \mathbb{Z}^+$ is not divisible by any positive integer other than 1 and p itself, then p is said to be **prime**.

It is probably worth pointing out the elementary fact that if $a|b$ and $a|c$, then $a|(mb + nc)$ for any $m, n \in \mathbb{Z}$. This is because $a|b$ implies $b = q_1a$, and $a|c$ implies $c = q_2a$. Thus $mb + nc = (mq_1 + nq_2)a$ so that $a|(mb + nc)$.

Theorem 0.8 (**Division Algorithm**) If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, then there exist unique integers q and r such that $a = qb + r$ where $0 \le r < b$.

Proof Define $S = \{a - nb \ge 0: n \in \mathbb{Z}\}$. In other words, S consists of all nonnegative integers of the form $a - bn$. It is easy to see that $S \neq \varnothing$. Indeed, if $a \ge 0$ we simply choose $n = 0$ so that $a \in S$, and if $a < 0$ we choose $n = a$ so that $a - ba = a(1 - b) \in S$ (since $a < 0$ and $1 - b \le 0$). Since S is a nonempty subset of the natural numbers, we may apply the well-ordering property of the natural numbers to conclude that S contains a least element $r \ge 0$. If we let q be the value of n corresponding to this r, then we have $a - qb = r$ or $a = qb + r$ where $0 \le r$. We must show that $r < b$. To see this, suppose that $r \ge b$. Then

$$a - (q + 1)b = a - qb - b = r - b \ge 0$$

so that $a - (q + 1)b \in S$. But $b > 0$ so that

$$a - (q + 1)b = (a - qb) - b < a - qb = r$$

which contradicts the definition of r as the least element of S. Hence $r < b$.

To prove uniqueness, we suppose that we may write $a = q_1b + r_1$ and $a = q_2b + r_2$ where $0 \le r_1 < b$ and $0 \le r_2 < b$. Equating these two formulas yields $q_1b + r_1 = q_2b + r_2$ or $(q_1 - q_2)b = r_2 - r_1$, and therefore $b|(r_2 - r_1)$. Using the fact that $0 \le r_1 < b$ and $0 \le r_2 < b$, we see that $r_2 - r_1 < b - r_1 \le b$. Similarly we have $r_1 - r_2 < b - r_2 \le b$ or $-b < r_2 - r_1$. This means that $-b < r_2 - r_1 < b$. Therefore $r_2 - r_1$ is a multiple of b that lies strictly between $-b$ and b, and thus we must have $r_2 - r_1 = 0$. Then $(q_1 - q_2)b = 0$ with $b \neq 0$, and hence $q_1 - q_2 = 0$ also. This shows that $r_1 = r_2$ and $q_1 = q_2$ which completes the proof of uniqueness. ∎

Suppose we are given two integers $a, b \in \mathbb{Z}$ where we assume that a and b are not both zero. We say that an integer $d \in \mathbb{Z}^+$ is the **greatest common divisor** of a and b if $d|a$ and $d|b$, and if c is any other integer with the property that $c|a$ and $c|b$, then $c|d$. We denote the greatest common divisor of a and b by $\gcd\{a, b\}$. Our next theorem shows that the gcd always exists and is unique. Furthermore, the method of proof shows us how to actually compute the gcd.

Theorem 0.9 (**Euclidean Algorithm**) If a, b $\in \mathbb{Z}$ are not both zero, then there exists a unique positive integer d $\in \mathbb{Z}^+$ such that

(a) d|a and d|b.

(b) If c $\in \mathbb{Z}$ is such that c|a and c|b, then c|d.

Proof First assume b > 0. Applying the division algorithm, there exist unique integers q_1 and r_1 such that

$$a = q_1 b + r_1 \quad \text{with } 0 \le r_1 < b \; .$$

If $r_1 = 0$, then b|a and we may take d = b to satisfy both parts of the theorem. If $r_1 \ne 0$, then we apply the division algorithm again to b and r_1, obtaining

$$b = q_2 r_1 + r_2 \quad \text{with } 0 \le r_2 < r_1 \; .$$

Continuing this procedure, we obtain a sequence of nonzero remainders r_1, r_2, . . . , r_k where

$$\begin{aligned} a &= q_1 b + r_1 && \text{with} \quad 0 \le r_1 < b \\ b &= q_2 r_1 + r_2 && \text{with} \quad 0 \le r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 && \text{with} \quad 0 \le r_3 < r_2 \\ &\;\vdots && \qquad\qquad\qquad\qquad\qquad\qquad (*) \\ r_{k-2} &= q_k r_{k-1} + r_k && \text{with} \quad 0 \le r_k < r_{k-1} \\ r_{k-1} &= q_{k+1} r_k \end{aligned}$$

That this process must terminate with a zero remainder as shown is due to the fact that each remainder is a nonnegative integer with $r_1 > r_2 > \cdots$. We have denoted the last nonzero remainder by r_k.

We now claim that d = r_k. Since $r_{k-1} = q_{k+1} r_k$, we have $r_k | r_{k-1}$. Then, because $r_{k-2} = q_k r_{k-1} + r_k$ and $r_k | r_k$ and $r_k | r_{k-1}$, we have $r_k | r_{k-2}$. Continuing in this manner, we see that $r_k | r_{k-1}$, $r_k | r_{k-2}$, . . . , $r_k | r_1$, r_k|b and r_k|a. This shows that r_k is a common divisor of a and b. To show that r_k is in fact the greatest common divisor, we first note that if c|a and c|b, then c|r_1 because $r_1 = a - q_1 b$. But now we see in the same way that c|r_2, and working our way through the above set of equations we eventually arrive at c|r_k. Thus r_k is a gcd as claimed.

If b < 0, we repeat the above process with a and −b rather than a and b. Since b and −b have the same divisors, it follows that a gcd of {a, −b} will be a gcd of {a, b} (note we have not yet shown the uniqueness of the gcd). If b = 0, then we can simply let d = |a| to satisfy both statements in the theorem.

As to uniqueness of the gcd, suppose we have integers d_1 and d_2 that satisfy both statements of the theorem. Then applying part (b) to both d_1 and d_2, we must have $d_1|d_2$ and $d_2|d_1$. But both d_1 and d_2 are positive, and hence $d_1 = d_2$. ∎

Corollary If $d = \gcd\{a, b\}$ where a and b are not both zero, then $d = am + bn$ for some $m, n \in \mathbb{Z}$.

Proof Referring to equations (*) in the proof of Theorem 0.9, we note that the equation for r_{k-2} may be solved for r_k to obtain $r_k = r_{k-2} - r_{k-1}\, q_k$. Next, the equation $r_{k-3} = q_{k-1}r_{k-2} + r_{k-1}$ may be solved for r_{k-1}, and this is then substituted into the previous equation to obtain $r_k = r_{k-2}(1 + q_{k-1}q_k) - r_{k-3}\, q_k$. Working our way up equations (*), we next eliminate r_{k-2} to obtain r_k in terms of r_{k-3} and r_{k-4} . Continuing in this manner, we eventually obtain r_k in terms of b and a. ∎

If $a, b \in \mathbb{Z}$ and $\gcd\{a, b\} = 1$, then we say that a and b are **relatively prime** (or sometimes **coprime**). The last result on integers that we wish to prove is the result that if p is prime and $p|ab$ (where $a, b \in \mathbb{Z}$), then either $p|a$ or $p|b$.

Theorem 0.10 (a) Suppose $a, b, c \in \mathbb{Z}$ where $a|bc$ and a and b are relatively prime. Then $a|c$.

(b) If p is prime and $a_1, \dots, a_n \in \mathbb{Z}$ with $p|a_1 \cdots a_n$, then $p|a_i$ for some $i = 1, \dots, n$.

Proof (a) By the corollary to Theorem 0.9 we have $\gcd\{a, b\} = 1 = am + bn$ for some $m, n \in \mathbb{Z}$. Multiplying this equation by c we obtain $c = amc + bnc$. But $a|bc$ by hypothesis so clearly $a|bnc$. Since it is also obvious that $a|amc$, we see that $a|c$.

(b) We proceed by induction on n, the case $n = 1$ being trivial. We therefore assume that $n > 1$ and $p|a_1 \cdots a_n$. If $p|a_1 \cdots a_{n-1}$, then $p|a_i$ for some $i = 1, \dots, n - 1$ by our induction hypothesis. On the other hand, if $p\nmid a_1 \cdots a_{n-1}$ then $\gcd\{p, a_1, \dots, a_{n-1}\} = 1$ since p is prime. We then apply part (a) with $a = p$, $b = a_1 \cdots a_{n-1}$ and $c = a_n$ to conclude that $p|a_n$. ∎

Exercises

1. Find the gcd of the following sets of integers:
   (a) {6, 14}.
   (b) {−75, 105}.
   (c) {14, 21, 35}.

2. Find the gcd of each set and write it in terms of the given integers:
(a) $\{1001, 33\}$.
(b) $\{-90, 1386\}$.
(c) $\{-2860, -2310\}$.

3. Suppose p is prime and $p \nmid a$ where $a \in \mathbb{Z}$. Prove that a and p are relatively prime.

4. Prove that if $\gcd\{a, b\} = 1$ and $c|a$, then $\gcd\{b, c\} = 1$.

5. If $a, b \in \mathbb{Z}^+$, then $m \in \mathbb{Z}^+$ is called the **least common multiple** (abbre–viated lcm) if $a|m$ and $b|m$, and if $c \in \mathbb{Z}$ is such that $a|c$ and $b|c$, then $m|c$. Suppose $a = p_1^{s_1} \cdots p_k^{s_k}$ and $b = p_1^{t_1} \cdots p_k^{t_k}$ where $p_1, \ldots, p_k$ are distinct primes and each s_i and t_i are ≥ 0.
(a) Prove that $a|b$ if and only if $s_i \leq t_i$ for all $i = 1, \ldots, k$.
(b) For each $i = 1, \ldots, k$ let $u_i = \min\{s_i, t_i\}$ and $v_i = \max\{s_i, t_i\}$. Prove that $\gcd\{a, b\} = p_1^{u_1} \cdots p_k^{u_k}$ and $\mathrm{lcm}\{a, b\} = p_1^{v_1} \cdots p_k^{v_k}$.

6. Prove the **Fundamental Theorem of Arithmetic**: Every integer > 1 can be written as a unique (except for order) product of primes. Here is an outline of the proof:
(a) Let $S = \{a \in \mathbb{Z}: a > 1$ and a can not be written as a product of primes.$\}$ (In particular, note that S contains no primes.) Show that $S = \varnothing$ by assuming the contrary and using the well-ordered property of the natural numbers.
(b) To prove uniqueness, assume that $n > 1$ is an integer that has two different expansions as $n = p_1 \cdots p_s = q_1 \cdots q_t$ where all the p_i and q_j are prime. Show that $p_1|q_j$ for some $j = 1, \ldots, t$ and hence that $p_1 = q_j$. Thus p_1 and q_j can be canceled from each side of the equation. Continue this argument to cancel one p_i with one q_j, and then finally concluding that $s = t$.

CHAPTER 1

An Introduction to Groups

While we have no intention of presenting a comprehensive treatment of group theory in this text, there are a number of definitions that will facilitate a rigorous description of vector spaces. Furthermore, the concepts from abstract algebra that we shall introduce will be of great use to us throughout the text.

1.1 DEFINITIONS

A **group** (G, •) is a nonempty set G together with a binary operation called **multiplication** (or a **product**) and denoted by • that obeys the following axioms:

(G1) $a, b \in G$ implies $a•b \in G$ (closure);
(G2) $a, b, c \in G$ implies $(a•b)•c = a•(b•c)$ (associativity);
(G3) There exists $e \in G$ such that $a•e = e•a = a$ for all $a \in G$ (identity);
(G4) For each $a \in G$, there exists $a^{-1} \in G$ such that $a•a^{-1} = a^{-1}•a = e$ (inverse).

Furthermore, a group is said to be **abelian** if it also has the property that

(G5) $a•b = b•a$ for all $a, b \in G$ (commutativity).

In the case of abelian groups, the group multiplication operation is frequently denoted by + and called **addition**. We will generally simplify our notation by leaving out the group multiplication symbol and assuming that it is understood for the particular group under discussion.

The number of elements in a group G is called its **order** of and will be denoted by o(G). (The order of G is frequently denoted by |G| although we shall not use this notation.) If this number is finite, then we say that G is a **finite** group. Otherwise, G is said to be **infinite**.

While we have defined a group in the usual manner, it should be realized that there is a certain amount of redundancy in our definition. In particular, it is not necessary to require that a "right inverse" also be the "left inverse." To see this, suppose that for any $a \in G$, we have the **right inverse** defined by $aa^{-1} = e$. Then multiplying from the left by a^{-1} yields $a^{-1}aa^{-1} = a^{-1}$. But $a^{-1} \in G$ so there exists an $(a^{-1})^{-1} \in G$ such that $(a^{-1})(a^{-1})^{-1} = e$. Multiplying our previous expression from the right by $(a^{-1})^{-1}$ results in $a^{-1}a = e$, and hence we see that a^{-1} is also a **left inverse**. Of course, we could have started with a left inverse and shown that it is also a right inverse.

Similarly, we could have defined a **right identity** by $ae = a$ for all $a \in G$. We then observe that $a = ae = a(a^{-1}a) = (aa^{-1})a = ea$, and hence e is also a **left identity**.

It is easy to show that the identity element is unique. To see this, suppose that there exist $e, \hat{e} \in G$ such that for every $a \in G$ we have $ea = ae = \hat{e}a = a\hat{e} = a$. Since $ea = a$ for every $a \in G$, we have in particular that $e\hat{e} = \hat{e}$. On the other hand, since we also have $a\hat{e} = a$, it follows that $e\hat{e} = e$. Therefore $\hat{e} = e\hat{e} = e$ so that $e = \hat{e}$.

Before showing the uniqueness of the inverse, we first prove an important basic result. Suppose that $ax = ay$ for $a, x, y \in G$. Let a^{-1} be a (not necessarily unique) inverse to a. Then $x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = ey = y$. In other words, the equation $ax = ay$ means that $x = y$. This is sometimes called the (left) **cancellation law**. As a special case, we see that $aa^{-1} = e = a\hat{a}^{-1}$ implies $a^{-1} = \hat{a}^{-1}$ so that the inverse is indeed unique as claimed. This also shows that

$$(a^{-1})^{-1} = a$$

since $(a^{-1})^{-1}(a^{-1}) = e$ and $aa^{-1} = e$.

Finally, another important result follows by noting that $(ab)(b^{-1}a^{-1}) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$. Since the inverse is unique, we then see that

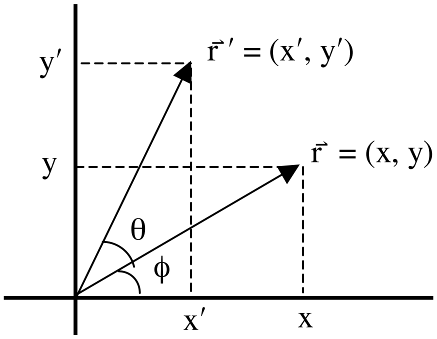
$$(ab)^{-1} = b^{-1}a^{-1} .$$

This clearly extends by induction to any finite product of group elements.

Example 1.1 The set of integers $\mathbb{Z} = 0, \pm 1, \pm 2, \ldots$ forms an infinite abelian group where the group multiplication operation is just ordinary addition. It should be obvious that the (additive) identity element is 0, and the inverse of any number n is given by −n. However, it is easy to see that $\mathbb{Z}$ is not a group under the operation of ordinary multiplication. Indeed, while $\mathbb{Z}$ is both closed and associative under multiplication, and it also contains the (multiplicative) identity element 1, no element of $\mathbb{Z}$ (other than ±1) has a multiplicative inverse in $\mathbb{Z}$ (for example, $2^{-1} = 1/2 \notin \mathbb{Z}$).

On the other hand, if we consider the set $\mathbb{Q}$ of all rational numbers, then $\mathbb{Q}$ forms a group under ordinary addition (with identity element 0 and inverse $-p/q \in \mathbb{Q}$ to any $p/q \in \mathbb{Q}$). Moreover, the *nonzero* elements of $\mathbb{Q}$ also form a group under ordinary multiplication (with identity element 1 and inverse $q/p \in \mathbb{Q}$ to any $p/q \in \mathbb{Q}$). ∕∕

Example 1.2 A more complicated (but quite useful) example is given by the set of all rotations in the xy-plane. (This example uses some notation that we have not yet defined in this book, although most readers should have no difficulty following the discussion.) Consider the following figure that shows a vector $\vec{r} = (x, y)$ making an angle ϕ with the x-axis, and a vector $\vec{r}\,' = (x', y')$ making an angle $\theta + \phi$ with the x-axis:



We assume $r = |\vec{r}| = |\vec{r}\,'|$ so that the vector $\vec{r}\,'$ results from a counterclockwise rotation by an angle θ with respect to the vector $\vec{r}$. From the figure, we see that $\vec{r}\,'$ has components x' and y' given by

$$x' = r\cos(\theta+\phi) = r\cos\theta\cos\phi - r\sin\theta\sin\phi = x\cos\theta - y\sin\theta$$
$$y' = r\sin(\theta+\phi) = r\sin\theta\cos\phi + r\cos\theta\sin\phi = x\sin\theta + y\cos\theta.$$

Let $R(\alpha)$ denote a counterclockwise rotation by an angle α. It should be clear that $R(0)$ is just the identity rotation (i.e., no rotation at all), and that the inverse is given by $R(\alpha)^{-1} = R(-\alpha)$. With these definitions, it is easy to see that the set of all rotations in the plane forms an infinite (actually, continuous) abelian group. A convenient way of describing these rotations is with the matrix

$$R(\alpha) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

(Such a matrix is said form a **representation** of the rotation group.) We then see that $\vec{r}' = R(\theta)\,\vec{r}$, which in matrix notation is just

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Using this notation, it is easy to see that R(0) is the identity since

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

and also that $R(\theta)^{-1} = R(-\theta)$ because

$$R(\theta)R(-\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = R(-\theta)R(\theta).$$

We remark that while the rotation group in two dimensions is abelian, the rotation group in three dimensions is not. For example, let $R_z(\theta)$ denote a rotation about the z-axis (in the "right-handed sense"). Then, applied to any vector $\hat{x}$ lying along the x-axis, we see that

$$R_y(90^\circ)R_z(45^\circ)\hat{x} \neq R_z(45^\circ)R_y(90^\circ)\hat{x}$$

since in the second case, the result lies along the z-axis, while in the first case it does not. ∕∕

While we will return shortly to discuss subgroups in more detail, it will be of use to define them now. If G is a group, then a subset $H \subset G$ is said to be a subgroup of G if the elements of H form a group under the same group multiplication rule as G. For example, the set $\mathbb{Z}$ of integers is a subgroup of the group $\mathbb{Q}$ of all rational numbers under ordinary addition. Furthermore, it is easy to show that a nonempty subset H of a group G is a subgroup of G if and only if $a, b \in H$ implies that $ab \in H$, and $a \in H$ implies that $a^{-1} \in H$ (see Exercise 1.1.9).

Exercises

1. Decide which of the following sets G forms a group under the indicated operation. If G does not form a group, give the reason.
   (a) G = {all integers} under ordinary subtraction.
   (b) G = {all nonzero rational numbers} under ordinary division.
   (c) G = {a_0, a_1, . . . , a_6} where

$$a_i a_j = \begin{cases} a_{i+j} & \text{if } i+j<7 \\ a_{i+j-7} & \text{if } i+j \geq 7 \end{cases}.$$

   (d) G = {$2^m 3^n$: m, n ∈ ℤ} under ordinary multiplication.

2. Let F denote the set of all mappings from ℝ into ℝ. For any f, g ∈ F we define (f + g)(x) = f(x) + g(x) for each x ∈ ℝ so that f + g ∈ F. Show that this defines a group.

3. Show that the collection of all subsets of a set S, with the operation of taking symmetric differences (see Exercise 0.1.2) as the group multiplication operation, forms a group. [*Hint*: Show that the identity element is ∅, and the inverse of any A ⊂ S is A itself.]

4. Prove that any group of order n ≤ 4 must be abelian.

5. Given two groups A and B, we can form the Cartesian product A × B = {(a, b): a ∈ A and b ∈ B} of these groups considered as sets. Prove that A × B can be made into a group with respect to the operation defined by (a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2) for all a_1, a_2 ∈ A and b_1, b_2 ∈ B. This group is called the **direct product** of A and B.

6. Prove that {(x, x): x ∈ G} is a subgroup of G × G (see the previous problem). This is called the **diagonal subgroup** of G × G.

7. Let G = {g_1, . . . , g_n} be a group, and let h ∈ G be arbitrary but fixed. Define the set hG = {hg_1, . . . , hg_n} = {g_{h_1}, . . . , g_{h_n}}. Show that hG = G, and conclude that the ordered set (h_1, . . . , h_n) is a permutation of the ordered set (1, . . . , n). (This simple but very useful result is frequently referred to as the **rearrangement lemma**.)

8. Let H be a subgroup of a group G.

(a) If e is the identity element in G and f is the identity element in H, show that f = e.
(b) If a ∈ H, show that the inverse element a^{-1} is the same in H as the a^{-1} is in G.

9. Let H be a nonempty subset of a group G. Prove that H is a subgroup of G if and only if a, b ∈ H implies ab ∈ H and a ∈ H implies $a^{-1} \in H$.

10. Let $\mathcal{H}$ be a collection of subgroups of a group G. Show that the intersection of all $H \in \mathcal{H}$ is a subgroup of G.

11. Let G be a group. An element a ∈ G is said to be **conjugate** to an element b ∈ G if there exists g ∈ G such that $b = gag^{-1}$. Show that this defines an equivalence relation on G. (Mutually conjugate elements of G are said to form a (conjugate) **class**.)

12. Let X be a (nonempty) subset of a group G, and let $\{H_i\colon i \,\varepsilon\, I\}$ be the collection of all subgroups of G that contain X. Then $\cap H_i$ is called the **subgroup** of G **generated by the set X** and denoted ⟨X⟩. Prove that ⟨X⟩ consists of *all* finite products $a_1^{n_1} a_2^{n_2} \cdots a_r^{n_r}$ where $a_i \in X$ and $n_i \in \mathbb{Z}$. [*Hint* : Show that the set H of *all* such products is a subgroup of G that contains X and is contained in every subgroup containing X. Thus H < ⟨X⟩ < H.]

1.2 PERMUTATION GROUPS

Let G be any group and suppose a ∈ G. As a matter of notational convenience, we define $a^0 = e$, $a^1 = a$, $a^2 = aa$, . . . , $a^k = aa^{k-1}$, as well as $a^{-2} = (a^{-1})^2$, $a^{-3} = (a^{-1})^3$, . . . (where a^{-1} is the usual inverse element to a). It is then easy to see that for any m, n ∈ ℤ we have $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$. From now on we will assume the reader understands that this is what is meant when we write an element of any group to a power.

Now consider three objects (, Δ, O) where the parentheses mean that the given order is relevant. We define this to be the **canonical** (or standard) order on the set {, Δ, O}. Given any other ordered triple, for example (O, , Δ), we define a **permutation** f of the set S = {, Δ, O} by

$$f = \begin{pmatrix} \square & \Delta & O \\ O & \square & \Delta \end{pmatrix}$$

where the first line is the set of objects in their canonical order and the second line is the given order. In other words, a **permutation** on a set S is a bijection from S onto itself. Note that simply giving an arbitrary order to a collection of objects does not in itself define a permutation. It is necessary that some canonical order also be specified as a point of reference.

This notation, where the top row *defines* the canonical order, is referred to as **two-line** notation. However, it is very important to realize that as long as the same pairing of objects is maintained between the top and bottom rows, we may rearrange these pairs any way we please. For example, the above permutation f can equally well be written as

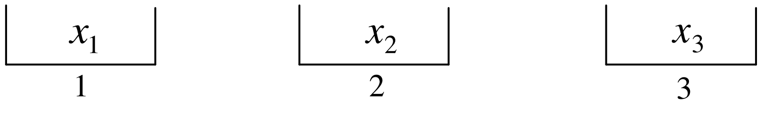
$$f = \begin{pmatrix} \mathrm{O} & \square & \Delta \\ \Delta & \mathrm{O} & \square \end{pmatrix}.$$

It is also common to use a simplified **one-line** notation. In this case, the canonical order must be understood. For example, in the first case above we would write simply f = (O, , Δ) where the canonical order is understood to be (, Δ, O).

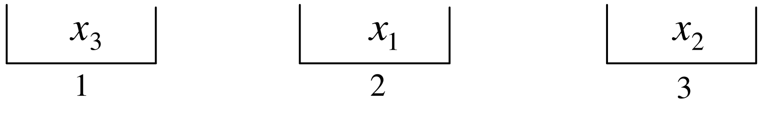
While we have now given a precise definition of the term “permutation,” there are other ways of describing permutations that are very useful in practice. Two of these are given in the next (rather long) example, which will then be generalized to form one of the most useful groups in linear algebra.

Example 1.3 Suppose we have three boxes that each contain a single object. Now, given three distinct objects and three boxes, any one of the three objects could go into the first box, then either of the two remaining objects could go into the second box, and finally only the remaining object can go into the third and last box. In other words, there are 3! = 6 possible placements of the three distinct objects in the three boxes such that each box receives a single object. Let us see how permutations can be used to describe the distribution of distinct objects among boxes. We give two common, intuitive interpretations.

Imagine three boxes labelled 1, 2, 3 that contain objects x_1, x_2, x_3 respectively, as shown below:



We now redistribute these objects among the boxes as follows:



One way to describe the transition from the first distribution to the second is by the permutation

$$\tilde{f} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

which is to be interpreted as a rule for redistributing objects by saying "take the object in box i (a number in the upper row) and place it in box $\tilde{f}$ (i) (the number in the lower row directly below it)." In this example, this means that we take the object in box i = 1 and place it in box $\tilde{f}$ (1) = 2, the object in box i = 2 goes into box $\tilde{f}$ (2) = 3, and the object in box i = 3 goes into box $\tilde{f}$ (3) = 1. This rule yields the second distribution from the first.

(Note also that in terms of our original definition of a permutation, we can interpret $\tilde{f}$ as a reordering of boxes in space. In other words, we can equally well describe the above redistribution in effect by leaving the objects fixed in space and rearranging the boxes underneath them. It is easy to see that if we leave the objects in the order (x_1, x_2, x_3) and label the boxes underneath them in the order (2, 3, 1), then we obtain the same pairing of objects and boxes.)

Another approach to describing this transition is by using permutations on the set of objects. For example, if we let

$$f = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix}$$

then the second distribution (the lower row) is obtained from the first distribution (the upper row) by interpreting f as "replace object x_1 (wherever it is) by object x_3 , replace object x_2 (wherever it is) by object x_1 , and replace object x_3 (wherever it is) by object x_2." An equivalent way to describe this permutation is by the mapping f defined by

$$f(x_1) = x_3$$
$$f(x_2) = x_1$$
$$f(x_3) = x_2$$

which we can write in the simple one-line notation

$$f = (x_3, x_1, x_2).$$

Let us denote the set of objects {x_1, x_2, x_3} by S. Since there are only six possible distinct arrangements of S within the three boxes, there can be only six such permutations of S. We wish to make this set of permutations into a group. In particular, we will then have a group (denoted by S_3) of permutations defined on the set S. This group is called the **symmetric group** (or the **permutation group**) of **degree** 3. Since S_3 contains 3! = 6 elements, its order is 6.

We define the group multiplication as the composition of our permutations. For example, consider the permutation in S_3 defined by either

$$\tilde{g} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

or

$$g = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}$$

which in our one-line notation is simply $g = (x_2, x_1, x_3)$. Composing this with the above permutation $f = (x_3, x_1, x_2)$ we have, for example,

$$(fg)(x_1) = f(g(x_1)) = f(x_2) = x_1$$

and it is easy to see that the complete expression is given by $fg = (x_1, x_3, x_2)$. Note however, that

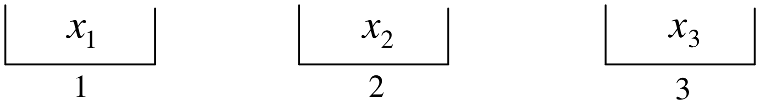
$$gf = (x_3, x_2, x_1) \neq fg$$

so that S_3 is a nonabelian group. This composition of mappings also shows us how to multiply our permutations. Indeed, if we write out the equation $fg = (x_1, x_3, x_2)$ in terms of our two-line notation, we obtain

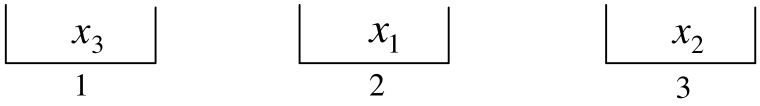
$$fg = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix}.$$

Reading the product from right to left, we first see that x_1 is replaced by x_2, and then this x_2 is replaced by x_1, and the net result is that x_1 is replaced by x_1. Next we see that x_2 is first replaced by x_1, and then this x_1 is replaced by x_3 with the net result of replacing x_2 by x_3. Finally, x_3 is replaced by x_3, and then this x_3 is replaced by x_2, resulting in the replacement of x_3 by x_2. Therefore we see that combining the product from right to left results in exactly the same permutation as shown on the right hand side.

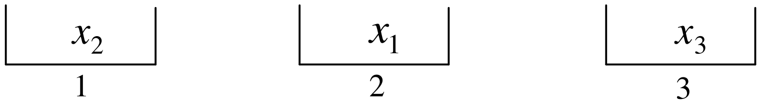
Now let us see how to combine the alternative descriptions in terms of $\tilde{f}$ and $\tilde{g}$. We know that $\tilde{f}$ takes the initial distribution



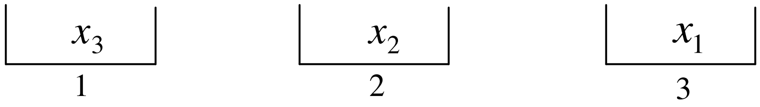
to the redistributed form (“contents of box 1 to box 2, contents of box 2 to box 3, and contents of box 3 to box 1”)



and $\tilde{g}$ takes the initial distribution to the redistributed form



Applying $\tilde{f}$ to this last distribution we obtain (just take the contents of box 1 to box 2 etc.)



With respect to the initial distribution, this composition of permutations is just the permutation

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

In other words, simply following each permutation in sequence results in

$$\tilde{f}\tilde{g} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Again reading the product from right to left, we see that the object in box 1 goes into box 2, and then the object in box 2 goes into box 3, with the net result that the object in box 1 goes into box 3. Next, the object in box 2 goes into box 1, and then the object in box 1 goes into box 2, resulting in the object in box 2 going into box 2. Finally, the object in box 3 goes into box 3, and then the object in box 3 goes into box 1, resulting in the object in box 3 going into box 1. Therefore, reading this type of product from right to left also results in the correct combination of permutations.

We now observe that $f^2(x_1) = f(x_3) = x_2$, and in general

$$f^2 = (x_2, x_3, x_1)$$

and

$$f^3 = (x_1, x_2, x_3)$$

which shows that $f^3 = ff^2 = e$, and hence $f^{-1} = f^2$. Similarly, we leave it to the reader to show that $g^2 = e$, and hence $g^{-1} = g$.

Since S_3 contains six elements and we have already constructed the six distinct mappings $\{e, f, g, f^2, fg, gf\}$, it must be true that any combination of mappings may be reduced to one of these six. To see this, all we really need to calculate is $(f^{-1}g)(x_1) = f^{-1}(x_2) = x_3$, and in general,

$$f^{-1}g = (x_3, x_2, x_1) = gf$$

so that $f^{-1}g = gf$. For example, we have $f(gf) = f(f^{-1}g) = (ff^{-1})g = g$. Other combinations are proved in a similar manner. ∕∕

We now generalize this example to the case of an arbitrary (but finite) number of elements. Let S be a set containing a finite number n of elements. Then the set S_n of all one-to-one mappings of S onto itself is called the **permutation group** of **degree** n. It should be clear that S_n is of order n!. If $f \in S_n$, then f has the effect of taking $x_i \rightarrow f(x_i)$ which we may write as

$$f = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_{i_1} & x_{i_2} & \cdots & x_{i_n} \end{pmatrix}$$

where $(i_1, \dots, i_n)$ is some permutation of $(1, \dots, n)$. To simplify our notation, let us write this mapping as

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

where the top row stands for $(x_1, x_2, \dots, x_n)$ and the bottom row represents $(x_{i_1}, x_{i_2}, \dots, x_{i_n})$ which is just $(x_1, \dots, x_n)$ in some permuted order. This should not be confused with the interpretation (which we will no longer use) of permutations as "the object in box 1 goes into box i_1" etc.

The identity element in S_n is

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

and the inverse to any given permutation is just the permutation that restores the original order. For instance, the inverse to the permutation f defined in Example 1.3 is the permutation $f^{-1} = f^2$ given in this notation by

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

In general, we will denote elements of S_n by Greek letters such as θ, ϕ and σ, so that we have expressions such as θx, $\theta^2 x = \theta\theta x$, and so forth. In other words, if $\theta \in S_3$ is just the mapping f in the previous example, then we would have $\theta 1 = 3$, $\theta 2 = 1$ and $\theta 3 = 2$.

Now let S be any set of n elements, and consider any element $\theta \in S_n$. Given any x, y ∈ S, we say that x is **equivalent** to y if $y = \theta^i x$ for some $i \in \mathbb{Z}$, and we write this as $x \approx_\theta y$. Since $x = \theta^0 x = ex = x$, we see that $x \approx_\theta x$. Next, note that if $x \approx_\theta y$, then $x = \theta^i y$ so that $y = \theta^{-i}x$, and hence $y \approx_\theta x$. In addition, if $x \approx_\theta y$ and $y \approx_\theta z$, then $x = \theta^i y = \theta^i \theta^j z = \theta^{i+j} z$, and hence $x \approx_\theta z$. We have therefore defined an equivalence relation on S as described in Section 0.3. Furthermore, Theorem 0.2 shows that this equivalence relation induces a decomposition of S into disjoint subsets called the equivalence classes of S.

For each x ∈ S, the equivalence class of x is the set $[x] = \{\theta^i x\colon i \in \mathbb{Z}\}$ which is called the **orbit** of x under θ. Since S is finite, sooner or later repeated applications of θ to x must give back x. In other words, for each x ∈ S there exists some smallest positive integer m such that $\theta^m x = x$ (where the value of m need not be the same for every x ∈ S). Thus the orbit of x under θ will be the set $\{x, \theta x, \dots, \theta^{m-1}x\}$. If we consider these elements as being in a particular order, we then obtain what is called a **cycle** of θ, and we write this as $(x, \theta x, \dots, \theta^{m-1}x)$. In words, this means "x is replaced by θx, θx is replaced by $\theta^2 x$, . . . , and $\theta^{m-1}x$ is replaced by x." It should be clear that a knowledge of all the cycles of θ is the same as knowing θ, because we would then know the result of applying θ to any x ∈ S. (While the cycle notation is the same as the one-line notation for a permutation, the context should always make it clear which is meant.)

Example 1.4 Let $S = \{x_1, \dots, x_6\}$ which we denote by $\{1, \dots, 6\}$ for simplicity. We consider the element $\theta \in S_6$ given by

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}.$$

Now observe that $\theta 1 = 2$ and $\theta^2 1 = \theta 2 = 1$, so the orbit of 1 is the set {1, 2} and the corresponding cycle is (1, 2). Since this cycle is the equivalence class of 1 and equivalence classes are disjoint, we see that it must also be the equivalence class of 2. Continuing, the orbit of 3 is just {3}, and for 4 we have $\theta 4 = 5$, $\theta^2 4 = 6$, and $\theta^3 4 = 4$ so that the orbit of 4 is {4, 5, 6}. Thus the cycles of θ are (1, 2), (3) and (4, 5, 6). Notice that these cycles are disjoint ordered equivalence classes of S under the mapping $\theta \in S_6$. ∕∕

We can carry this idea one step further as follows. Consider a cycle of the form $(i_1, \dots, i_m)$ which we now interpret as that permutation which replaces i_1 by i_2, i_2 by i_3, . . . , i_{m-1} by i_m, and i_m by i_1. For example, using the set S = {1, . . . , 6}, the cycle (2, 6, 3) is to be interpreted as the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 4 & 5 & 3 \end{pmatrix}.$$

Since we already know how to multiply permutations, we now have a way to multiply cycles. Thus, using this same S and, for example, the cycles (1, 5) and (2, 6, 3), we have

$$\begin{aligned}(1, 5)(2, 6, 3) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 4 & 1 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 4 & 5 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}.\end{aligned}$$

Note that while we have defined our multiplication as proceeding from right to left, in this case we would have obtained the same result by multiplying the cycles in either order. In fact, it should not be hard to convince yourself that this will always be the case when *disjoint* cycles are multiplied together. In other words, disjoint cycles commute. This is because each cycle only acts on a specific subset of elements that are not acted on by any other (disjoint) cycle.

As another example, let us now find the cycles of the permutation

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}.$$

We have θ1 = 5 and $\theta^2 1 = 1$ so that the orbit of 1 is {1, 5}. Also, θ2 = 6, $\theta^2 2 = 3$, and $\theta^3 2 = 2$ so the orbit of 2 is {2, 6, 3}. Therefore θ has the cycles (1, 5) and (2, 6, 3) (and of course, also (4)). But now notice that θ is just the product of these cycles (which contain no elements in common) taken in any order. A little thought as we just mentioned shows that this is not unexpected, as we prove in our first theorem.

Theorem 1.1 Every permutation can be expressed as the product of disjoint cycles.

Proof Consider any permutation $\theta \in S_n$ on a set S, and assume that θ has k cycles where each cycle is of the form $(x, \theta x, \theta^2 x, \ldots, \theta^{m_i-1}x)$ for some i with $1 \le i \le k$. (Note that since each $x \in S$ must be in some cycle, and since the cycles are disjoint, we must have $\Sigma_{i=1}^{k} m_i = n$ where n is the number of elements in S.) When these cycles are multiplied together, we see that each of the corresponding permutations affects only those elements contained in the orbit (i.e., cycle) it represents. Hence, by multiplying together all of the cycles, each element of S will be accounted for with the same result as θ.

Another way to see this is to consider the effect of θ on any $x \in S$. The resulting element θx is exactly the same as the image of x under the product of all the (disjoint) cycles of θ since only the cycle containing x will have any effect on it. Since both θ and the product of its cycles have the same effect on any $x \in S$, it must be true that θ equals the product of its cycles. ∎

At this point, there is no substitute for simply working out an example for yourself. Thus, the reader should pick some permutation, find its cycles, and then multiply them together. In so doing, the proof of Theorem 1.1 should become quite obvious (or see the exercises at the end of this section).

Suppose that S = {1, 2, . . . , m} and consider the product of the 2-cycles (1, m), (1, m − 1), . . . , (1, 3), (1, 2). Expressing these in terms of their corresponding permutations, we have (note the order of factors since we are multiplying from right to left, and these cycles are not disjoint)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & m \\ m & 2 & 3 & 4 & \cdots & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & m \\ 3 & 2 & 1 & 4 & \cdots & m \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & m \\ 2 & 1 & 3 & 4 & \cdots & m \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & m \\ 2 & 3 & 4 & 5 & \cdots & 1 \end{pmatrix}.$$

But this last permutation is just the m-cycle (1, 2, . . . , m). A similar calculation shows that in fact any m-cycle of the form $(a_1, a_2, \ldots, a_m)$ may be written as the product $(a_1, a_m) \cdots (a_1, a_3)(a_1, a_2)$. (We remark that the multiplication of 2-cycles is one place where multiplying from left to right would be more natural.)

Example 1.5 Consider the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix}$$

and its cycle (1, 3, 2, 5). We claim that this cycle may be written as the product (1, 5)(1, 2)(1, 3). There are actually two equivalent ways of seeing this. First, we could write out all of the complete permutations as

$$(1, 3, 2, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 1 & 6 \end{pmatrix} \qquad (1, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix}$$

$$(1, 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 5 & 6 \end{pmatrix} \qquad (1, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 4 & 1 & 6 \end{pmatrix}$$

It is then easy to see that (1, 3, 2, 5) = (1, 5)(1, 2)(1, 3).

On the other hand, we could also leave out those elements in each permutation that are not affected by any of the cycles, and simply write

$$(1, 3, 2, 5) = \begin{pmatrix} 1 & 3 & 2 & 5 \\ 3 & 2 & 5 & 1 \end{pmatrix} \qquad (1, 3) = \begin{pmatrix} 1 & 3 & 2 & 5 \\ 3 & 1 & 2 & 5 \end{pmatrix}$$

$$(1, 2) = \begin{pmatrix} 1 & 3 & 2 & 5 \\ 2 & 3 & 1 & 5 \end{pmatrix} \qquad (1, 5) = \begin{pmatrix} 1 & 3 & 2 & 5 \\ 5 & 3 & 2 & 1 \end{pmatrix}$$

Again, we obtain (1, 3, 2, 5) = (1, 5)(1, 2)(1, 3). At this point you should be sufficiently familiar with the cycle notation to be able to multiply cycles without reverting to two-line notation. ∕∕

All of this discussion has shown that any m-cycle may be written as a product of 2-cycles, which are usually called **transpositions**. However we could also write, for example, (1, 2, . . . , m) = (m, m − 1) · · · (m, 2)(m, 1) so that this decomposition is by no means unique.

With all of this background, it is now easy to prove an important result in the description of permutations.

Theorem 1.2 Every permutation can be written as the product of transpositions.

Proof Theorem 1.1 showed that every permutation can be written as the product of disjoint cycles, while we just showed that any cycle can be written (in a non-unique manner) as the product of transpositions. ∎

In view of this theorem, we say that a permutation is **even** (**odd**) if it can be written as the product of an even (odd) number of transpositions. Of course, since the decomposition of cycles into transpositions is not unique, we must be sure that such a designation is unambiguous. This is the intent of our next theorem.

Theorem 1.3 If a permutation can be represented by an even (odd) number of transpositions in one decomposition, then any other decomposition must also be an even (odd) number of transpositions.

Proof Define the polynomial p in n real variables by

$$\begin{aligned} p(x_1,\ldots,x_n) &= \prod\nolimits_{i<j}(x_i - x_j) \\ &= (x_1 - x_2)(x_1 - x_3)\cdots(x_2 - x_3)(x_2 - x_4)\cdots(x_{n-1} - x_n) \end{aligned}$$

and let $\sigma \in S_n$ be any transposition. By σp we mean

$$\sigma p(x_1, \ldots, x_n) = p(x_{\sigma 1}, \ldots, x_{\sigma n}) \ .$$

We claim that $\sigma p = -p$. To see this in detail, let σ be the transposition (x_a, x_b). We assume without loss of generality that $x_a < x_b$, and write out all of those terms in $p(x_1, \ldots, x_n)$ that contain either x_a or x_b (or both). Thus, those terms containing x_a are

$$\underbrace{\{(x_1 - x_a)(x_2 - x_a)\cdots(x_{a-1} - x_a)\}}_{a-1 \text{ terms}}$$

$$\times\underbrace{\{(x_a - x_{a+1})(x_a - x_{a+2})\cdots(x_a - x_{b-1})\}}_{b-a-1 \text{ terms}}$$

$$\times\underbrace{\{(x_a - x_b)\}}_{1 \text{ term}}\times\underbrace{\{(x_a - x_{b+1})\cdots(x_a - x_n)\}}_{n-b \text{ terms}}$$

while those containing x_b are

$$\underbrace{\{(x_1 - x_b)(x_2 - x_b)\cdots(x_{a-1} - x_b)\}}_{a-1 \text{ terms}}\times\underbrace{\{(x_a - x_b)\}}_{\substack{\text{already}\\ \text{counted}}}$$

$$\times\underbrace{\{(x_{a+1} - x_b)(x_{a+2} - x_b)\cdots(x_{b-1} - x_b)\}}_{b-a-1 \text{ terms}}$$

$$\times\underbrace{\{(x_b - x_{b+1})\cdots(x_b - x_n)\}}_{n-b\text{ terms}}$$

Since all of these terms are multiplied together, we see that if x_a and x_b are interchanged (but *not* x_{a+1} and x_{b+1} etc.), there will be no net effect on the polynomial $p(x_1, \ldots, x_n)$ except for the unpaired term $(x_a - x_b)$ which results in a single change of sign. This shows that $\sigma p = -p$ as claimed.

Now, for any other $\theta \in S_n$, Theorem 1.2 shows that $\theta = \prod_i \sigma_i$ where each σ_i is a transposition. Thus, if

$$\theta = \prod_{i=1}^{k} \sigma_i$$

we see that

$$\theta p = \left(\prod_{i=1}^{k} \sigma_i\right) p = (-1)^k p.$$

Similarly, if

$$\theta = \prod_{i=1}^{m} \sigma_i$$

we have $\theta p = (-1)^m p$. Therefore, if θ is represented by k transpositions and by m transpositions, we must have $(-1)^k p = (-1)^m p$, and hence k and m must both be even or both be odd. ∎

This result allows us to make the unambiguous definition of the sign of a permutation as follows. We define the sign of a permutation θ, sgn θ, by

$$\operatorname{sgn}\theta = \begin{cases} +1 \text{ if } \theta \text{ is even} \\ -1 \text{ if } \theta \text{ is odd} \end{cases}.$$

Our next theorem will be of great benefit to us when we come to discuss the theory of determinants in Chapter 4.

Theorem 1.4 For any two permutations $\theta, \phi \in S_n$ we have

$$\operatorname{sgn}(\theta\phi) = (\operatorname{sgn}\theta)(\operatorname{sgn}\phi) .$$

Proof By Theorem 1.2, we may write θ as a product of k transpositions and ϕ as a product of m transpositions. Therefore it follows from Theorem 1.3 that $\operatorname{sgn}\theta = (-1)^k$ and $\operatorname{sgn}\phi = (-1)^m$. But then

$$\operatorname{sgn}(\theta\phi) = (-1)^{k+m} = (-1)^k(-1)^m = (\operatorname{sgn}\theta)(\operatorname{sgn}\phi) \ . \ ∎$$

As the final topic in our treatment of permutations, we take a look at the inverse of a given transposition. For any given transposition (a_1, a_2), it should be obvious that $(a_1, a_2)^2$ is just the identity transposition. This may be formally shown by noting that

$$(a_1, a_2)^2 = (a_1, a_2)(a_1, a_2) = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}\begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix} = e.$$

Since the identity element in any group is unique, this means that for any transposition σ we have $\sigma^{-1} = \sigma$. In view of this result, one might rightfully expect that the sign of an inverse permutation is the same as the sign of the permutation itself.

Theorem 1.5 For any $\theta \in S_n$ we have $\operatorname{sgn}\theta^{-1} = \operatorname{sgn}\theta$.

Proof By Theorem 1.2, we write $\theta = \sigma_1\sigma_2 \cdots \sigma_m$ where each σ_i is a transposition. Then, using the fact that θ is just a product of elements in the group S_2 , we see that

$$\theta^{-1} = (\sigma_1 \sigma_2 \cdots \sigma_m)^{-1} = \sigma_m{}^{-1} \cdots \sigma_2{}^{-1} \sigma_1{}^{-1} = \sigma_m \cdots \sigma_2 \sigma_1$$

and hence $\operatorname{sgn}\theta^{-1} = (-1)^m = \operatorname{sgn}\theta$. ∎

Exercises

1. Consider the following permutations

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \qquad \phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

and compute each of the following:

(a) $\theta\phi$ (b) $\phi\theta$ (c) θ^{-1} (d) ϕ^{-1}
(e) $\theta^{-1}\phi^{-1}$ (f) $\phi^{-1}\theta^{-1}$ (g) $(\theta\phi)^{-1}$ (h) $(\phi\theta)^{-1}$

2. Referring to Example 1.3, evaluate $gfgf^3gf$. How is $\tilde{f}$ related to f?

3. Find all of the orbits and cycles of the following permutations:

$(a)\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}.$

$(b)\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}.$

4. Express each of the following as the product of disjoint cycles:
(a) (1, 2, 3)(4, 5)(1, 6, 7, 8, 9)(1, 5)
(b) (1, 2)(1, 2, 3)(1, 2)

5. Determine which of the following products of cycles is an even permutation:
(a) (1, 2, 3)(1, 2)
(b) (1, 2, 3, 4, 5)(1, 2, 3)(4, 5)
(c) (1, 2)(1, 3)(1, 4)(2, 5)

6. Show that the set $A_n \subset S_n$ consisting of *even* permutations forms a group. Show that S_n consists of n!/2 even permutations and n!/2 odd permutations.

7. Compute $\theta^{-1}\phi\theta$ for each of the following:
(a) $\theta = (1, 3, 5)(1, 2)$ $\qquad \phi = (1, 5, 7, 9)$.
(b) $\theta = (5, 7, 9)$ $\qquad \phi = (1, 2, 3)$.

8. Show that permutations with the same cycle structure belong to the same class (see Exercise 1.1.8). In other words, if $\theta, \phi \in S_n$, show that $\theta\phi\theta^{-1}$ has the same cycle structure as ϕ. [*Hint*: Using two-line notation, show that $\theta\phi\theta^{-1}$ may be evaluated by simply applying θ to the top and bottom rows of ϕ separately.]

9. Show that S_n is non-abelian if $n \geq 3$.

1.3 HOMOMORPHISMS OF GROUPS

We now turn our attention to a discussion of mappings from one group to another. These results will be absolutely fundamental to everything else that follows, and it is essential that the reader thoroughly understand the concepts to be presented in this section.

Let $\phi\colon G \to G'$ be a mapping from a group G to a group G'. If for every $x, y \in G$ we have

$$\phi(xy) = \phi(x)\,\phi(y)$$

then ϕ is said to be a **homomorphism**, and the groups G and G' are said to be **homomorphic**. In other words, a homomorphism preserves group multiplication, but is not in general either surjective or injective. It should also be noted that the product xy is an element of G while the product $\phi(x)\,\phi(y)$ is an element of G'.

Example 1.6 Let G be the (abelian) group of all real numbers under addition, and let G' be the group of nonzero real numbers under multiplication. If we define $\phi\colon G \to G'$ by $\phi(x) = 2^x$, then

$$\phi(x + y) = 2^{x+y} = 2^x\, 2^y = \phi(x)\,\phi(y)$$

so that ϕ is indeed a homomorphism. ∕∕

Example 1.7 Let G be the group of all real (or complex) numbers under ordinary addition. For any real (or complex) number a, we define the mapping ϕ of G onto itself by $\phi(x) = ax$. This ϕ is clearly a homomorphism since

$$\phi(x + y) = a(x + y) = ax + ay = \phi(x) + \phi(y)\ .$$

However, if b is any other nonzero real (or complex) number, then we leave it to the reader to easily show that the ("nonhomogeneous") mapping $\psi(x) = ax + b$ is not a homomorphism. ∕∕

Let e be the identity element of G, and let e' be the identity element of G'. If $\phi\colon G \to G'$ is a homomorphism, then $\phi(x)e' = \phi(x) = \phi(xe) = \phi(x)\phi(e)$, and we have the important result

$$\phi(e) = e'.$$

Using this result, we then see that $e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\,\phi(x^{-1})$, and hence the uniqueness of the inverse tells us that

$$\phi(x^{-1}) = \phi(x)^{-1} .$$

It is very important to note that in general $\phi(x)^{-1} \neq \phi^{-1}(x)$ since if $x \in G$ we have $\phi(x)^{-1} \in G'$ while if $x \in G'$, then $\phi^{-1}(x) \in G$. Using these results, it should now be easy for the reader to show that $\phi(G)$ forms a subgroup of G' (see Exercise 1.3.1).

In general, there may be many elements $x \in G$ that map into the same element $x' \in G'$ under ϕ. It is of particular interest to see what happens if more than one element of G (besides e) maps into e'. If $k \in G$ is such that $\phi(k) = e'$, then for any $x \in G$ we have $\phi(xk) = \phi(x)\,\phi(k) = \phi(x)e' = \phi(x)$. Therefore if $xk \neq x$ we see that ϕ could not possibly be a one-to-one mapping. To help us get a hold on when a homomorphism is one-to-one, we define the **kernel** of ϕ to be the set

$$\operatorname{Ker} \phi = \{x \in G: \phi(x) = e'\} .$$

It is also easy to see that Ker ϕ is a subgroup of G (see Exercise 1.3.1).

If a homomorphism $\phi: G \rightarrow G'$ is one-to-one (i.e., injective), we say that ϕ is an **isomorphism**. If, in addition, ϕ is also onto (i.e., surjective), then we say that G and G' are **isomorphic**. In other words, G and G' are isomorphic if ϕ is a bijective homomorphism. (We point out that many authors use the word "isomorphism" to implicitly mean that ϕ is a bijection.) In particular, an isomorphism of a group onto itself is called an **automorphism**.

From the definition, it appears that there is a relationship between the kernel of a homomorphism and whether or not it is an isomorphism. We now proceed to show that this is indeed the case. By way of notation, if H is a subset of a group G, then by Hg we mean the set $Hg = \{hg \in G: h \in H\}$. Recall also that if $\phi: G \rightarrow G'$ and $x' \in G'$ then, by an inverse image of x', we mean any element $x \in G$ such that $\phi(x) = x'$.

Theorem 1.6 Let ϕ be a homomorphism of a group G onto a group G', and let K_ϕ be the kernel of ϕ. Then given any $x' \in G'$, the set of all inverse images of x' is given by $K_\phi\, x$ where $x \in G$ is any particular inverse image of x'.

Proof Consider any $k \in K_\phi$. Then by definition of homomorphism, we must have

$$\phi(kx) = \phi(k)\,\phi(x) = e'x' = x' .$$

In other words, if x is any inverse image of x', then so is any $kx \in K_\phi\, x$. We must be sure that there is no other element $y \in G$, $y \notin K_\phi\, x$ with the property that $\phi(y) = x'$.

To see that this is true, suppose $\phi(y) = x' = \phi(x)$. Then $\phi(y) = \phi(x)$ implies that

$$e' = \phi(y)\phi(x)^{-1} = \phi(y)\phi(x^{-1}) = \phi(yx^{-1}) \ .$$

But this means that $yx^{-1} \in K_\phi$, and hence $yx^{-1} = k$ for some $k \in K_\phi$. Therefore $y = kx \in K_\phi\, x$ and must have already been taken into account. ∎

Corollary A homomorphism ϕ mapping a group G to a group G′ is an isomorphism if and only if $\operatorname{Ker} \phi = \{e\}$.

Proof Note that if $\phi(G) \neq G'$, then we may apply Theorem 1.6 to G and $\phi(G)$. In other words, it is trivial that ϕ always maps G *onto* $\phi(G)$. Now, if ϕ is an isomorphism, then it is one-to-one by definition, so that there can be no element of G other than e that maps into e′. Conversely, if $\operatorname{Ker} \phi = \{e\}$ then Theorem 1.6 shows that any $x' \in \phi(G) \subset G'$ has exactly one inverse image. ∎

Of course, if ϕ is surjective, then $\phi(G)$ is just equal to G′. In other words, we may think of isomorphic groups as being essentially identical to each other.

Example 1.8 Let G be any group, and let $g \in G$ be fixed. We define the mapping $\phi\colon G \rightarrow G$ by $\phi(x) = gxg^{-1}$, and we claim that ϕ is an automorphism. To see this, first note that ϕ is indeed a homomorphism since for any $x, y \in G$ we have

$$\begin{aligned}\phi(xy) &= g(xy)g^{-1} = g(xey)g^{-1} = g(xg^{-1}gy)g^{-1} = (gxg^{-1})(gyg^{-1})\\ &= \phi(x)\phi(y).\end{aligned}$$

To see that ϕ is surjective, simply note that for any $y \in G$ we may define $x = g^{-1}yg$ so that $\phi(x) = y$. Next, we observe that if $\phi(x) = gxg^{-1} = e$, then right-multiplying by g and left multiplying by g^{-1} yields

$$x = (g^{-1}g)x(g^{-1}g) = g^{-1}eg = e$$

and hence $\operatorname{Ker} \phi = \{e\}$. From the corollary to Theorem 1.6, we now see that ϕ must be an isomorphism. ∕∕

Exercises

1. Let ϕ: G → G′ be a homomorphism.
   (a) Show that $\phi(G)$ is a subgroup of G′.
   (b) Show that Ker ϕ is a subgroup of G.

2. Show that the composition $\phi \circ \psi$: A → C is a homomorphism if both ϕ: B → C and ψ: A → B are.

3. Determine which of the following mappings ϕ: G → G′ are homomorphisms, and for those that are, determine their kernel:
   (a) G = G′ = the group of nonzero real numbers under multiplication, and $\phi(x) = x^2$ for all $x \in G$.
   (b) Repeat part (a) but with $\phi(x) = 2^x$.
   (c) G = G′ = the group of all real numbers under addition, and $\phi(x) = 1 + x$ for all $x \in G$.
   (d) Repeat part (c), but with $\phi(x) = kx$ for any (fixed) number k.

4. Show that an isomorphism ϕ defines an equivalence relation on the set of all groups.

5. If G is abelian and G′ is isomorphic to G, prove that G′ is also abelian.

6. Let $\mathbb{R}^+$ denote the set of all real numbers > 0, and define the mapping ϕ: $\mathbb{R}^+ \to \mathbb{R}$ by $\phi(x) = \log_{10} x$ for each $x \in \mathbb{R}^+$. Let $\mathbb{R}^+$ be a group with respect to multiplication, and let $\mathbb{R}$ be a group with respect to addition. Show that ϕ is an isomorphism.

7. Let A and B be groups (with their own group operations). Show that A × B is isomorphic to B × A (see Exercise 1.1.5).

8. (a) (**Cayley's theorem**) Prove that every group G of order n is isomorphic to a subgroup of S_n for some S. [*Hint*: By the rearrangement lemma (Exercise 1.1.7), we know that hG = G for any $h \in G$. If $G = \{g_1, \ldots, g_n\}$, define the mapping ψ: G → S_n by

$$\psi(a) = \begin{pmatrix} g_1 & \cdots & g_n \\ ag_1 & \cdots & ag_n \end{pmatrix}$$

for every $a \in G$. Using the techniques of Exercise 1.2.8, show that ψ is a homomorphism, i.e., $\psi(ab) = \psi(a)\psi(b)$.]

(b) Explain why this result shows that there can only be a finite number of non-isomorphic groups of order n.

1.4 RINGS AND FIELDS

Before starting our discussion of vector spaces, let us first define precisely what is meant by a field. We shall see that this is simply a generalization of those essential properties of the real and complex numbers that we have been using all along. For the sake of completeness and future reference, we will do this in a somewhat roundabout manner.

A nonempty set R together with two operations denoted by + and • is said to be an **associative ring** if it obeys the following axioms for all a, b, c $\in$ R:

(R1) $a + b \in R$;
(R2) $a + b = b + a$;
(R3) $(a + b) + c = a + (b + c)$;
(R4) There exists an element $0 \in R$ such that $a + 0 = a$;
(R5) There exists and element $-a \in R$ such that $a + (-a) = 0$;
(R6) $a•b \in R$;
(R7) $(a•b)•c = a•(b•c)$;
(R8) $a•(b + c) = a•b + a•c$ and $(a + b)•c = a•c + b•c$.

Since every ring that we will ever discuss obeys (R7), we henceforth drop the adjective "associative" when discussing rings. It should also be noticed that (R1) – (R5) simply require that R be an abelian group under the operation + which we call addition. In addition to these axioms, if there exists an element $1 \in R$ such that $a•1 = 1•a = a$ for every $a \in R$, then R is said to be a **ring with unit element**. Furthermore, if for every a, b $\in$ R we have $a•b = b•a$, then R is called a **commutative ring**. As usual, we shall generally leave out the multiplication sign when dealing with rings.

Example 1.9 The set $\mathbb{Z}$ of all real integers under the usual operations of addition and multiplication is a commutative ring with unit element. However, the set of even integers under addition and multiplication is a commutative ring with no unit element. Note also that the set $\mathbb{Z}^+$ of positive integers is not a ring since there are no additive inverse (i.e., negative) elements in this set. ∕∕

Note that while the elements of a ring form an additive abelian group, we have not required that each element have a multiplicative inverse. However, if the nonzero elements of a ring R happen to form a group under multiplication, we say that R is a **division ring**. In this case we denote the unit element of R by 1, and we let a^{-1} denote the inverse of any element $a \in R$. The reason that only the nonzero elements are considered is that 0 has no inverse 0^{-1} such that $0 \bullet 0^{-1} = 1$. Finally, a **field** is defined to be a commutative division ring. We will generally denote an arbitrary field by the symbol $\mathcal{F}$.

Example 1.10 It should be clear that the real numbers $\mathbb{R}$ form a field with the usual operations of addition and multiplication. However, the set $\mathbb{Z}$ of integers does not form a field because for any $n \in \mathbb{Z}$ with $n \neq 0$, we have $n^{-1} = 1/n \quad \mathbb{Z}$ (except for $n = \pm 1$).

It is also true that the complex numbers $\mathbb{C}$ form a field, but this is slightly more difficult to prove. To do so, let us denote a complex number a + ib by the ordered pair $(a, b) \in \mathbb{R} \times \mathbb{R}$. Referring to Section 0.6 for motivation, we define addition and multiplication on these pairs by

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d)\\(a, b)(c, d) &= (ac - bd, ad + bc)\end{aligned}$$

for all $a, b, c, d \in \mathbb{R}$. We claim that the set $\mathbb{C}$ consisting of all such ordered pairs is a field. Some of the details will be left to the reader to fill in, but we will show the important points here. The additive identity element is clearly (0, 0), the negative of any $(a, b) \in \mathbb{C}$ is $(-a, -b)$, and the multiplicative identity is (1, 0). Multiplication is commutative since

$$(a, b)(c, d) = (ac - bd, ad + bc) = (ca - db, cb + da) = (c, d)(a, b)\,.$$

To prove associativity, we have

$$\begin{aligned}(a, b)[(c, d)(e, f)] &= (a, b)(ce - df, cf + de)\\&= (ace - adf - bcf - bde, acf + ade + bce - bdf)\\&= (ac - bd, ad + bc)(e, f)\\&= [(a, b)(c, d)](e, f).\end{aligned}$$

Finally, we show that every $(a, b) \neq (0, 0)$ has an inverse in $\mathbb{C}$. Since a and b can not both be 0, we have $a^2 + b^2 > 0$. We leave it to the reader to show that

$$(a, b)\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = (1, 0).$$

(In the notation of Chapter 0, we see that this is just the statement that $zz^* = |z|^2$ implies $z^{-1} = z^*/|z|^2$.)

We will be using the fields $\mathbb{R}$ and $\mathbb{C}$ almost exclusively in this text. //

Since we will be using fields (and therefore rings) as our usual number system, let us use the defining relations to prove formally that a ring behaves in the manner we are accustomed to and expect.

Theorem 1.7 Let R be a ring with unit element. Then for all $a, b \in R$ we have

(a) $a0 = 0a = 0$.
(b) $a(-b) = (-a)b = -(ab)$.
(c) $(-a)(-b) = ab$.
(d) $(-1)a = -a$.
(e) $(-1)(-1) = 1$.

Proof (a) $a0 = a(0 + 0)$ (by (R4)) $= a0 + a0$ (by (R8)). But R is an additive abelian group, so that canceling $a0$ from both sides of this equation says that $a0 = 0$. Similarly, we see that $0a = (0 + 0)a = 0a + 0a$ implies $0a = 0$.

(b) $ab + a(-b) = a(b + (-b))$ (by (R8)) $= a0$ (by (R5)) $= 0$ (by (a)). Therefore the group property of R shows that $a(-b) = -(ab)$. It is clear that we also have $(-a)b = -(ab)$.

(c) $(-a)(-b) = -(a(-b))$ (by (b)) $= -(-(ab))$ (by (b) again). But $-(-(ab))$ is the unique inverse to $-(ab)$, and since we also have $ab + (-(ab)) = 0$, it follows that $-(-(ab)) = ab$.

(d) $a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0$ so that $(-1)a = -a$.

(e) This follows from (d) using $a = -1$ since $(-1)(-1) = -(-1) = 1$. ∎

Note the fact that R contains a unit element was actually only required for parts (d) and (e) of this theorem.

Exercises

1. Let R be a ring. Prove that $a^2 - b^2 = (a + b)(a - b)$ and that $(a + b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$ if and only if R is commutative (where by terms of the form a^2 we mean aa).

2. Let F denote the set of all mappings from $\mathbb{R}$ into $\mathbb{R}$. For any $f, g \in F$, we define $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for each $x \in \mathbb{R}$. In other words, $f + g$ and fg are in F. Show that this defines a ring of functions.

3. In the previous problem, show that if we replace the product fg by the composition $f \circ g$ then this does not define a ring.

4. Show that the set $\mathbb{Q}$ of all rational numbers forms a field.

5. Consider the set $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}: a, b \in \mathbb{Z}\}$. We define addition and multiplication in $\mathbb{Z}[\sqrt{2}]$ by

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

and

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} \ .$$

Show that the set $\mathbb{Z}[\sqrt{2}]$ with these operations forms a ring. Does it form a field?

6. Repeat the previous problem with $\mathbb{Q}$ instead of $\mathbb{Z}$.

1.5 MORE ON GROUPS AND RINGS

In this section we lay the foundation for future work in our chapter on polynomials. If the reader has not had much experience with abstract algebra, this section may prove somewhat long and difficult on a first reading. Because of this, the student should feel free to skim this section now, and return to it only when it becomes necessary in later chapters.

We have seen that fields offer a distinct advantage over rings in that elements of the field can be divided (since the field contains the multiplicative inverse of each nonzero element). It will be of interest to know how certain rings can be "enlarged" to form a field. Rather than treat this problem directly, we choose to introduce some additional terminology that will be of use in discussing further properties of polynomials.

In view of the fact that a ring has both addition and multiplication defined on it, we make the following definition. Let R and R′ be rings. A mapping $\phi: R \rightarrow R'$ is said to be a **ring homomorphism** if

$$\phi(a + b) = \phi(a) + \phi(b)$$

and

$$\phi(ab) = \phi(a)\,\phi(b)$$

for all a, b ∈ R. We see that

$$\phi(a) = \phi(0 + a) = \phi(0) + \phi(a)$$

and therefore $\phi(0) = 0$. Then we also have

$$0 = \phi(a - a) = \phi(a) + \phi(-a)$$

so that adding $-\phi(a)$ to both sides yields

$$\phi(-a) = -\phi(a) \ .$$

While these last two results are the exact analogues of what we found for groups, not all of our results can be carried over directly. In particular, it must be remembered that every element of a group had an inverse in the group, while no such requirement is made on the multiplication in an arbitrary ring (recall that a ring in which the nonzero elements form a multiplicative group is called a division ring).

If R is a commutative ring, a nonzero element $a \in R$ is said to be a **zero divisor** if there exists a nonzero element $b \in R$ such that $ab = 0$. We then say that a commutative ring is an **integral domain** if it contains no zero divisors. For example, the ring of integers is an integral domain.

Example 1.11 Consider the set $\mathbb{Z}$ of all integers, and let $n \in \mathbb{Z}^+$ be fixed. A notation that is frequently used in algebra is to write $a|b$ to mean "a divides b," (i.e., in this case, that b is an integral multiple of a) and $c\nmid d$ to mean "c does not divide d." We define a relationship between the integers a and b by writing

$$a \equiv b(\text{mod } n)$$

if $n|(a - b)$. This relation is called **congruence modulo n**, and we read it as "a is congruent to b modulo n." We leave it as an exercise for the reader to show that this defines an equivalence relation on the set of integers (see Exercise 1.5.2). For example, it should be clear that $5 = 2(\text{mod } 3)$, $23 = 5(\text{mod } 6)$ and $21 = -9(\text{mod } 10)$.

Now suppose we define a ring R to be the set of integers mod 6 (this ring is usually denoted by $\mathbb{Z}_6$). Then the elements of R are the equivalence classes of the integers, and we denote the equivalence class of an integer n by [n]. Then the elements of R are [0], [1], [2], [3], [4] and [5]. For example, from the previous paragraph we see that [5] = [23] because $6|(23 - 5)$.

We define addition in R by [a] + [b] = [a + b], and thus [0] is the zero element of R. Defining multiplication in R by [a][b] = [ab], we see, for example, that $[2][5] = [4]$. However, note that $[2][3] = [0]$ even though $[2] \neq [0]$ and $[3] \neq [0]$, and thus R is not an integral domain. We will have much more to say about this ring in Section 6.6. ∕∕

It should now be clear that arbitrary rings can have a number of properties that we generally find rather unpleasant. Another type of pathology that is worth pointing out is the following. Let D be an integral domain. We say that D is of **finite characteristic** if there exists some integer $m > 0$ and some nonzero $a \in D$ such that $ma = 0$. Then the smallest positive integer p such that $pa = 0$ for some nonzero $a \in D$ is called the **characteristic** of D.

If D is an integral domain of characteristic p, then there exists a nonzero element $a \in D$ such that $pa = 0$. Then for any $x \in D$ we also have

$$0 = (pa)x = (a + \cdots + a)x = ax + \cdots + ax = a(x + \cdots + x) = a(px) .$$

But D has no zero divisors, and hence we must have $px = 0$ for every $x \in D$. If D has a unit element , then an equivalent requirement is to say that if D is of characteristic p, then $1 + \cdots + 1 = 0$, where there are p terms in the sum. Furthermore, any such sum consisting of less than p terms is nonzero.

Obviously, the most important types of integral domain for our purposes are those of characteristic 0. In other words, to say that D is of characteristic 0 means that if m is an integer and $a \in D$ is nonzero, then $ma = 0$ if and only if $m = 0$. The reason that we even bother to mention this is because most of the theory of matrices and determinants that we shall develop is valid over an arbitrary field $\mathcal{F}$. For example, we shall obtain results such as $\det A = -\det A$ which implies that $2 \det A = 0$. However, if $\mathcal{F}$ happens to be of characteristic 2, then we can not conclude from this that $\det A = 0$. In this book, we will always assume that our fields are of characteristic 0 (except in Section 6.6).

Returning to our general discussion, let 1 and $1'$ be the multiplicative identities of the rings R and R' respectively, and consider any ring homomorphism $\phi: R \rightarrow R'$. Then

$$\phi(a) = \phi(1a) = \phi(1)\,\phi(a)$$

but this does *not* in general imply that $\phi(1) = 1'$. However, if R' is an integral domain and $\phi(a) \neq 0$, then we have

$$0 = \phi(a) - \phi(1)\,\phi(a) = \phi(a)[1' - \phi(1)]$$

and hence $\phi(1) = 1'$ (note that we do not distinguish in our notation between 0 and $0'$).

As was the case with groups, we define the kernel of ϕ to be the set

$$\operatorname{Ker}\phi = \{a \in R: \phi(a) = 0\} \;.$$

If a, b ∈ Ker ϕ then

$$\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$$

so that a + b ∈ Ker ϕ also. Furthermore, if a ∈ Ker ϕ then

$$\phi(-a) = -\phi(a) = 0$$

so that the (additive) inverse of a is also in Ker ϕ. Thus Ker ϕ forms a subgroup of R under addition.

As we also did with groups, we say that a ring homomorphism of R into R′ is a (**ring**) **isomorphism** if it is an injective (i.e., one-to-one) mapping. If there exists a bijective ring homomorphism of R onto R′, then we say that R and R′ are isomorphic. Theorem 1.6 also carries over directly to the present case, and we then have that a ring homomorphism is an isomorphism if and only if Ker $\phi = \{0\}$.

Now note that another very important property of Ker ϕ comes from the observation that if a ∈ Ker ϕ and r ∈ R, then

$$\phi(ar) = \phi(a)\,\phi(r) = 0\phi(r) = 0 \;.$$

Similarly $\phi(ra) = 0$, and therefore both ar and ra are in Ker ϕ. We take this property as the prototype of a new object defined as follows.

A nonempty subset I of a ring R is said to be a (two-sided) **ideal** of R if I is a subgroup of R under addition, and if ar ∈ I and ra ∈ I for *all* a ∈ I and *all* r ∈ R. It is important to realize that the element r can be any element of R, not just an element of I.

Now let R be a *commutative* ring with unit element, and let a ∈ R be arbitrary. We denote by (a) the set of all multiples of a by elements of R. (While this is a somewhat confusing notation, it nevertheless conforms to standard usage.) In other words,

$$(a) = \{ra: r \in R\} \;.$$

We claim that (a) is actually an ideal of R. Indeed, if r, s ∈ R, then ra, sa ∈ (a) and therefore ra + sa = (r + s)a ∈ (a). Next, we have 0 = 0a ∈ (a), and finally, the negative (i.e., additive inverse) of ra ∈ (a) is (−r)a which is also in (a). This shows that (a) is a subgroup of R under addition. Lastly, for any ra ∈ (a) and any s ∈ R, we see that (ra)s = s(ra) = (sr)a ∈ (a). We have thus shown that (a) is an ideal. In general, any ideal of the form (a) is called a **principal** ideal, and the element $a \in R$ is called a **generator** of (a). A principal ideal (a) is thus the smallest ideal of R that contains a.

Example 1.12 We show that any field $\mathcal{F}$ has no ideals other than (0) and $\mathcal{F}$. Since the ideal (0) is quite trivial, let I be an ideal and assume that $I \neq (0)$. If $a \in I$, $a \neq 0$, then $a \in \mathcal{F}$ implies that $a^{-1} \in \mathcal{F}$ so that $1 = aa^{-1} \in I$ by the definition of ideal. But now, for any $r \in \mathcal{F}$ we have $r = 1r \in I$ (again by the definition of ideal), and hence $I = \mathcal{F}$. ∕∕

The converse of this example is given in the next theorem. Recall that a field is a commutative division ring, and hence a commutative ring R with unit element 1 is a field if every nonzero $a \in R$ has an inverse $b \in R$ with $ab = 1$.

Theorem 1.8 If R is a commutative ring with unit element whose only ideals are (0) and R, then R is a field.

Proof Part of this was proved in the above discussion, but for the sake of completeness we repeat it here. Let $a \in R$ be nonzero, and consider the set

$$Ra = \{ra : r \in R\} \ .$$

We shall first show that this set is an ideal of R. To see this, suppose $x, y \in Ra$. Then there exist $r_1, r_2 \in R$ such that $x = r_1a$ and $y = r_2a$. But then (using the definition of a ring) we see that

$$x + y = r_1a + r_2a = (r_1 + r_2)a \in Ra \ .$$

Next we note that

$$-x = -r_1a = (-r_1)a \in Ra$$

and therefore Ra is a subgroup of R under addition. Now, given any $r \in R$ we have

$$rx = r(r_1a) = (rr_1)a \in Ra$$

and since R is commutative, it also follows that $xr \in Ra$. This shows that Ra is an ideal of R.

By hypothesis, we see that Ra must equal either (0) or R. Since R is a ring with unit element, we have $0 \neq a = 1a \in Ra$ and hence $Ra \neq (0)$. This means that we must have $Ra = R$ so that every element of R is a multiple of a. In particular, since $1 \in R$, there must exist an element $b \in R$ with the property that $ba = 1$. In other words, $b = a^{-1}$ and thus R is a field. ∎

Now let H be a subgroup of a group G, and let $a \in G$ be arbitrary. Then the set

$$Ha = \{ha: h \in H\}$$

is called a **right coset** of H in G. Let $a, b \in G$ be arbitrary, and suppose that the cosets Ha and Hb have an element in common. This means that $h_1a = h_2b$ for some $h_1, h_2 \in H$. But then using the fact that H is a subgroup, we see that

$$a = h_1^{-1}h_1a = h_1^{-1}h_2b \in Hb \ .$$

Since this means that $a = hb$ for some $h = h_1^{-1}h_2 \in H$, we see (using the rearrangement lemma of Exercise 1.1.7) that this implies

$$Ha = Hhb = Hb$$

and therefore if any two right cosets have an element in common, then they must in fact be identical. It is easy to see that the set of all right cosets of H in G defines a partition of G and hence an equivalence relation that decomposes G into disjoint subsets (see Exercise 1.5.15).

Recall that o(G) denotes the order of G (i.e., the number of elements in the group G). We claim that if H is a subgroup of G, then $o(H) = o(Ha)$ for any $a \in G$. Indeed, to prove this we show that there is a bijection of H to Ha. Define the mapping $\alpha: H \rightarrow Ha$ by $\alpha(h) = ha$. This is clearly a surjective mapping since Ha consists precisely of elements of the form ha for $h \in H$. To see that it is also injective, suppose that for some $h_1, h_2 \in H$ we have $\alpha(h_1) = \alpha(h_2)$ or, equivalently, $h_1a = h_2a$. Multiplying from the right by a^{-1} then implies that $h_1 = h_2$, thus showing that α is one-to-one.

In the particular case of finite groups, the previous paragraph shows that any two right cosets of H in G must have the same number o(H) of elements. We also showed above that any two distinct right cosets have no elements in common. It then follows that any $a \in G$ is in the unique right coset Ha, and therefore the set of all right cosets of H in G must contain every element of G. This means that if there are k distinct right cosets of H in G, then we must have $ko(H) = o(G)$ (i.e., $o(H)|o(G)$), and hence we have proved **Lagrange's theorem**:

Theorem 1.9 If G is a finite group and H is a subgroup of G, then o(H) is a divisor of o(G).

The number o(G)/o(H) will be denoted by $i_G(H)$, and is usually called the **index** of H in G. (This is frequently denoted by [G : H].) The index of H in G is thus the number of distinct right cosets of H in G.

While we have restricted our discussion to right cosets, it is clear that everything could be repeated using **left cosets** defined in the obvious way. It should also be clear that for a general subgroup H of a group G, we need not have Ha = aH for any a ∈ G. However, if N is a subgroup of G such that for every n ∈ N and g ∈ G we have $gng^{-1} \in N$, then we say that N is a **normal** subgroup of G. An equivalent way of phrasing this is to say that N is a normal subgroup of G if and only if $gNg^{-1} \subset N$ for all g ∈ G (where by gNg^{-1} we mean the set of all gng^{-1} with n ∈ N).

Theorem 1.10 A subgroup N of G is normal if and only if $gNg^{-1} = N$ for every g ∈ G.

Proof If $gNg^{-1} = N$ for every g ∈ G, then clearly $gNg^{-1} \subset N$ so that N is normal. Conversely, suppose that N is normal in G. Then, for each g ∈ G we have $gNg^{-1} \subset N$, and hence

$$g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subset N \ .$$

Using this result, we see that

$$N = (gg^{-1})N(gg^{-1}) = g(g^{-1}Ng)g^{-1} \subset gNg^{-1}$$

and therefore $N = gNg^{-1}$ (This also follows from Example 1.8). ∎

The reader should be careful to note that this theorem does not say that $gng^{-1} = n$ for every n ∈ N and g ∈ G. This will in general not be true. The usefulness of this theorem is that it allows us to prove the following result.

Theorem 1.11 A subgroup N of G is normal if and only if every left coset of N in G is also a right coset of N in G.

Proof If N is normal, then $gNg^{-1} = N$ for every g ∈ G, and hence gN = Ng. Conversely, suppose that every left coset gN is also a right coset. We show that in fact this right coset must be Ng. Since N is a subgroup it must contain the identity element e, and therefore g = ge ∈ gN so that g must also be in whatever right coset it is that is identical to gN. But we also have eg = g so that g is in the right coset Ng. Then, since any two right cosets with an element in common must be identical, it follows that gN = Ng. Thus, we see that $gNg^{-1} = Ngg^{-1} = N$ so that N is normal. ∎

If G is a group and A, B are subsets of G, we define the set

$$AB = \{ab \in G: a \in A, b \in B\} .$$

In particular, if H is a subgroup of G, then $HH \subset H$ since H is closed under the group multiplication operation. But we also have $H = He \subset HH$ (since $e \in H$), and hence $HH = H$.

Now let N be a normal subgroup of G. By Theorem 1.11 we then see that

$$(Na)(Nb) = N(aN)b = N(Na)b = NNab = Nab .$$

In other words, the product of right cosets of a normal subgroup is again a right coset. This closure property suggests that there may be a way to construct a group out of the cosets Na where a is any element of G. We now show that there is indeed a way to construct such a group. Our method is used frequently throughout mathematics, and entails forming what is called a **quotient structure**.

Let G/N denote the collection of all right cosets of N in G. In other words, an element of G/N is a right coset of N in G. We use the product of subsets as defined above to define a product on G/N.

Theorem 1.12 Let N be a normal subgroup of a group G. Then G/N is a group.

Proof We show that the product in G/N obeys properties (G1) – (G4) in the definition of a group.

(1) If $A, B \in G/N$, then $A = Na$ and $B = Nb$ for some $a, b \in G$, and hence (since $ab \in G$)

$$AB = NaNb = Nab \in G/N .$$

(2) If $A, B, C \in G/N$, then $A = Na$, $B = Nb$ and $C = Nc$ for some $a, b, c \in G$ and hence

$$\begin{aligned}(AB)C &= (NaNb)Nc = (Nab)Nc = N(abN)c = N(Nab)c = N(ab)c \\ &= Na(bc) = Na(Nbc) = Na(NbNc) = A(BC).\end{aligned}$$

(3) If $A = Na \in G/N$, then

$$AN = NaNe = Nae = Na = A$$

and similarly

$$NA = NeNa = Nea = Na = A .$$

Thus $N = Ne \in G/N$ serves as the identity element in G/N.

(4) If $Na \in G/N$, then Na^{-1} is also in G/N, and we have

$$NaNa^{-1} = Naa^{-1} = Ne$$

as well as

$$Na^{-1}Na = Na^{-1}a = Ne \ .$$

Therefore $Na^{-1} \in G/N$ is the inverse to any element $Na \in G/N$. ∎

Corollary If N is a normal subgroup of a finite group G, then o(G/N) = o(G)/o(N).

Proof By construction, G/N consists of all the right cosets of N in G, and since this number is just the definition of $i_G(N)$, we see that o(G/N) = o(G)/o(N). ∎

The group defined in Theorem 1.12 is called the **quotient group** (or **factor group**) of G by N.

Let us now apply this quotient structure formalism to rings. Since any subgroup of an abelian group is automatically normal, and since any ring R is an abelian group under addition, any ideal I of R is therefore a normal subgroup of R (under addition). It is clear that we can now form the quotient group R/I where the elements of R/I are the cosets of I in R (since R is abelian, there is no need to distinguish between right and left cosets). We write these cosets as I + r (or r + I) for each $r \in R$. In the next theorem we show that R/I can in fact be made into a ring which is called the **quotient ring** of R by I.

Theorem 1.13 Let I be an ideal of a ring R. For any $I + a, I + b \in R/I$ we define

$$(I + a) + (I + b) = I + (a + b)$$

and

$$(I + a)(I + b) = I + ab \ .$$

Then, with these operations, R/I forms a ring.

Proof From the proof of Theorem 1.12, it is obvious that R/I forms a group under addition if we use the composition rule (I + a) + (I + b) = I + (a + b) for all $a, b \in R$. We now turn our attention to the multiplication rule on R/I, and we begin by showing that this rule is well-defined. In other words, we must show that if $I + a = I + a'$ and $I + b = I + b'$, then $I + ab = I + a'b'$. From $I + a = I + a'$, we have $a = x + a'$ for some $x \in I$, and similarly $b = y + b'$ for some $y \in I$. Then

$$ab = (x + a')(y + b') = xy + xb' + a'y + a'b' \ .$$

But I is an ideal so that xy, xb′, and a′y are all elements of I, and hence $z = xy + xb' + a'y \in I$. Therefore, $ab = z + a'b'$ so that

$$ab + I = a'b' + z + I = a'b' + I$$

as desired.

To show that R/I is a ring, we must verify that the properties (R1) – (R8) given in Section 1.4 hold in R/I. This is straightforward to do, and we give one example, leaving the rest to the reader (Exercise 1.5.5). To prove the first part of (R8), suppose $a, b, c \in R$. Then $I + a, I + b, I + c \in R/I$ and hence

$$\begin{aligned}(I + a)[(I + b) + (I + c)] &= (I + a)[I + (b + c)]\\ &= I + a(b + c)\\ &= I + (ab + ac)\\ &= (I + ab) + (I + ac)\\ &= (I + a)(I + b) + (I + a)(I + c).\end{aligned}$$

Example 1.13 Recall that the set $\mathbb{Z}$ of all integers forms a commutative ring with unit element (see Example 1.9). If we choose any $n \in \mathbb{Z}$, then n generates a principal ideal (n) that consists of all numbers of the form na for each $a \in \mathbb{Z}$. For example, the number 2 generates the principal ideal (2) that is nothing more than the ring of all even integers. The quotient ring $\mathbb{Z}/(2)$ is then the set of all cosets of (2). Each of these cosets is either the set of even integers, or the even integers plus some odd integer. ∕∕

We have now finished essentially all of the mathematical formalism necessary to undertake a rigorous study of linear algebra. In the next chapter we begin our treatment of the subject matter proper of this text.

Exercises

1. Let ϕ be a homomorphism of a group G into a group G′, and let K_ϕ be the kernel of ϕ. Prove that K_ϕ is a normal subgroup of G.

2. This exercise refers to the relation "congruence modulo n" defined in Example 1.11. Throughout this exercise, let $n \in \mathbb{Z}^+$ be arbitrary but fixed.
(a) Show that this relation defines an equivalence relation.
(b) Using Theorem 0.8 to divide a by n, show that the congruence relation has exactly n distinct equivalence sets.

(c) If $a \equiv b(\text{mod } n)$ and $c \equiv d(\text{mod } n)$, show that $a + c \equiv (b + d)(\text{mod } n)$ and $ac \equiv bd(\text{mod } n)$.
(d) Show $\mathbb{Z}/(n)$ is isomorphic to the integers mod n.

3. Let $\phi: R \to R'$ be a ring isomorphism. Show that R′ is commutative if R is.

4. Let $\phi: R \to R'$ be a ring isomorphism. Show that R′ is an integral domain if R is.

5. Finish the proof that R/I forms a ring in Theorem 1.13.

6. Prove that an integral domain is a field if and only if every nonzero element has a multiplicative inverse.

7. Show that the kernel of a ring homomorphism is an ideal.

8. Determine all the subgroups of the permutation group S_3. Which of these is normal?

9. Let $\mathcal{N}$ be a collection of normal subgroups of a group G. Show that the intersection of all $N \in \mathcal{N}$ is a normal subgroup of G.

10. Prove or disprove the following statement: If $\phi: R \to R'$ is a ring homomorphism, then the image of ϕ is an ideal of R′.

11. Let ϕ be a homomorphism of a group G onto a group G′, and let K be the kernel of ϕ. By Exercise 5.1, we know that K is a normal subgroup of G, and hence we may form the quotient group G/K. Prove that G/K is isomorphic to G′. [*Hint*: Since any element in $X \in G/K$ is of the form Kg where $g \in G$, define the mapping $\psi: G/K \to G'$ by $\psi(X) = \psi(Kg) = \phi(g)$. To show that ψ is an isomorphism, first show that ψ is well-defined, that is, $X = Kg = Kg'$ implies $\phi(g) = \phi(g')$. Next, show that ψ is a homomorphism, i.e., that $\psi(XY) = \psi(X)\,\psi(Y)$. Now show that ψ is surjective (use the fact that ϕ is surjective). Finally, show that $\text{Ker } \psi = \{0\}$ (you will need the additional fact that the identity in G/K is $K = Ke$).]

12. Show that a field $\mathcal{F}$ can have no zero divisors.

13. Let H be a subgroup of a group G. Show that the set of all right cosets of H in G decomposes G into disjoint subsets.

14. The center of a group G is the set $Z = \{z \in G\colon zg = gz \text{ for all } g \in G\}$. Show that Z is a normal subgroup of G.

15. Show that the set $\{0, 1\}$ with the usual addition and multiplication operations, but subject to $1 + 1 = 0$, forms a field of characteristic 2. (This is an example of a finite field.)

16. Let G be a group and let G_1, G_2 be subgroups of G with $G_1 \cap G_2 = e$. Show that G_1 and G_2 commute if and only if they are normal subgroups.

CHAPTER 2

Vector Spaces

We now begin our treatment of the principal subject matter of this text. We shall see that all of linear algebra is essentially a study of various transformation properties defined on a vector space, and hence it is only natural that we carefully define vector spaces. This chapter therefore presents a fairly rigorous development of (finite-dimensional) vector spaces, and a discussion of their most important fundamental properties. Basically, the general definition of a vector space is simply an axiomatization of the elementary properties of ordinary three-dimensional Euclidean space.

2.1 DEFINITIONS

A nonempty set V is said to be a **vector space** over a field $\mathcal{F}$ if: (i) there exists an operation called **addition** that associates to each pair x, y ∈ V a new vector x + y ∈ V called the **sum** of x and y; (ii) there exists an operation called **scalar multiplication** that associates to each a ∈ $\mathcal{F}$ and x ∈ V a new vector ax ∈ V called the **product** of a and x; (iii) these operations satisfy the following axioms:

(V1) $x + y = y + x$ for all x, y ∈ V.
(V2) $(x + y) + z = x + (y + z)$ for all x, y, z ∈ V.
(V3) There exists an element 0 ∈ V such that $0 + x = x$ for all x ∈ V.

(V4) For all $x \in V$ there exists an element $-x \in V$ such that $x + (-x) = 0$.
(V5) $a(x + y) = ax + ay$ for all $x, y \in V$ and all $a \in \mathcal{F}$.
(V6) $(a + b)x = ax + bx$ for all $x \in V$ and all $a, b \in \mathcal{F}$.
(V7) $a(bx) = (ab)x$ for all $x \in V$ and all $a, b \in \mathcal{F}$.
(V8) $1x = x$ for all $x \in V$ where 1 is the (multiplicative) identity in $\mathcal{F}$.

Note that (V1) – (V4) simply require that V be an additive abelian group. The members of V are called **vectors**, and the members of $\mathcal{F}$ are called scalars. The vector $0 \in V$ is called the **zero vector**, and the vector $-x$ is called the **negative** of the vector x.

We mention only in passing that if we replace the field $\mathcal{F}$ by an arbitrary ring R, then we obtain what is called an **R-module** (or simply a **module** over R). If R is a ring with unit element, then the module is called a **unital** R-module. In fact, this is the only kind of module that is usually considered in treatments of linear algebra. We shall not discuss modules in this text, although the interested reader can learn something about them from several of the books listed in the bibliography.

Throughout this chapter V will always denote a vector space, and the corresponding field $\mathcal{F}$ will be understood even if it is not explicitly mentioned. If $\mathcal{F}$ is the real field $\mathbb{R}$, then we obtain a **real vector space** while if $\mathcal{F}$ is the complex field $\mathbb{C}$, then we obtain a **complex vector space**. It may be easiest for the reader to first think in terms of these spaces rather than the more abstract general case.

Example 2.1 Probably the best known example of a vector space is the set $\mathcal{F}^n = \mathcal{F} \times \cdots \times \mathcal{F}$ of all n-tuples $(a_1, \dots, a_n)$ where each $a_i \in \mathcal{F}$. To make $\mathcal{F}^n$ into a vector space, we define the sum of two elements $(a_1, \dots, a_n) \in \mathcal{F}^n$ and $(b_1, \dots, b_n) \in \mathcal{F}^n$ by

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$

and scalar multiplication for any $k \in \mathcal{F}$ by

$$k(a_1, \dots, a_n) = (ka_1, \dots, ka_n) .$$

If $A = (a_1, \dots, a_n)$ and $B = (b_1, \dots, b_n)$, then we say that $A = B$ if and only if $a_i = b_i$ for each $i = 1, \dots, n$. Defining $0 = (0, \dots, 0)$ and $-A = (-a_1, \dots, -a_n)$ as the identity and inverse elements respectively of $\mathcal{F}^n$, the reader should have no trouble verifying properties (V1) – (V8).

The most common examples of the space $\mathcal{F}^n$ come from considering the fields $\mathbb{R}$ and $\mathbb{C}$. For instance, the space $\mathbb{R}^3$ is (with the Pythagorean notion of distance defined on it) just the ordinary three-dimensional Euclidean space (x, y, z) of elementary physics and geometry.

We shall soon see that any finite-dimensional vector space V over a field $\mathcal{F}$ is essentially the same as the space $\mathcal{F}^n$. In particular, we will prove that V is isomorphic to $\mathcal{F}^n$ for some positive integer n. ∕∕

Example 2.2 Another very useful vector space is the space $\mathcal{F}[x]$ of all polynomials in the indeterminate x over the field $\mathcal{F}$ (polynomials will be defined carefully in Chapter 6). In other words, every element in $\mathcal{F}[x]$ is a polynomial of the form $a_0 + a_1x + \cdots + a_nx^n$ where each $a_i \in \mathcal{F}$ and n is any positive integer (called the degree of the polynomial). Addition and scalar multiplication are defined in the obvious way by

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

and

$$c\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} (ca_i) x^i .$$

(If we wish to add together two polynomials $\sum_{i=0}^{n} a_ix^i$ and $\sum_{i=0}^{m} b_ix^i$ where $m > n$, then we simply define $a_i = 0$ for $i = n + 1, \dots, m$.)

Since we have not yet defined the multiplication of vectors, we ignore the fact that polynomials can be multiplied together. It should be clear that $\mathcal{F}[x]$ does indeed form a vector space. ∕∕

Example 2.3 We can also view the field $\mathbb{C}$ as a vector space over $\mathbb{R}$. In fact, we may generally consider the set of n-tuples $(x_1, \dots, x_n)$, where each $x_i \in \mathbb{C}$, to be a vector space over $\mathbb{R}$ by defining addition and scalar multiplication (by *real* numbers) as in Example 2.1. We thus obtain a real vector space that is quite distinct from the space $\mathbb{C}^n$. ∕∕

We now prove several useful properties of vector spaces that are analogous to the properties given in Theorem 1.7 for rings.

Theorem 2.1 Let V be a vector space over $\mathcal{F}$. Then for all $x, y, z \in V$ and every $a \in \mathcal{F}$ we have

(a) $x + y = z + y$ implies $x = z$.
(b) $ax = 0$ if and only if $a = 0$ or $x = 0$.
(c) $-(ax) = (-a)x = a(-x)$.

Proof We first remark that there is a certain amount of sloppiness in our notation since the symbol 0 is used both as an element of V and as an element of $\mathcal{F}$. However, there should never be any confusion as to which of these sets 0 lies in, and we will continue with this common practice.

(a) If x + y = z + y, then

$$(x + y) + (-y) = (z + y) + (-y)$$

implies

$$x + (y + (-y)) = z + (y + (-y))$$

which implies x + 0 = z + 0 and hence x = z. This is frequently called the (right) **cancellation law**. It is also clear that x + y = x + z implies y = z (left cancellation). (This is just a special case of the general result proved for groups in Section 1.1.)

(b) If a = 0, then

$$0x = (0 + 0)x = 0x + 0x \ .$$

But 0x = 0 + 0x so that 0 + 0x = 0x + 0x, and hence (a) implies 0 = 0x. If x = 0, then

$$a0 = a(0 + 0) = a0 + a0 \ .$$

But a0 = 0 + a0 so that 0 + a0 = a0 + a0, and again we have 0 = a0. Conversely, assume that ax = 0. If a ≠ 0 then a^{-1} exists, and hence

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}0 = 0$$

by the previous paragraph.

(c) By (V4) we have ax + (−(ax)) = 0, whereas by (b) and (V6), we have

$$0 = 0x = (a + (-a))x = ax + (-a)x \ .$$

Hence ax + (−(ax)) = ax + (−a)x implies −(ax) = (−a)x by (a). Similarly, 0 = x + (−x) so that

$$0 = a0 = a(x + (-x)) = ax + a(-x) \ .$$

Then 0 = ax + (−(ax)) = ax + a(−x) implies −(ax) = a(−x). ∎

In view of this theorem, it makes sense to define **subtraction** in V by

$$x - y = x + (-y) \ .$$

It should then be clear that a vector space will also have the properties we expect, such as a(x − y) = ax − ay, and −(x − y) = −x + y.

If we take an arbitrary subset of vectors in a vector space then, in general, this subset will not be a vector space itself. The reason for this is that in general, even the addition of two vectors in the subset will not result in a vector that is again a member of the subset. Because of this, we make the following definition. Suppose V is a vector space over $\mathcal{F}$ and $W \subset V$. Then if $x, y \in W$ and $c \in \mathcal{F}$ implies $x + y \in W$ and $cx \in W$, we say that W is a **subspace** of V. Indeed, if $c = 0$ then $0 = 0x \in W$ so that $0 \in W$, and similarly $-x = (-1)x \in W$ so that $-x \in W$ also. It is now easy to see that W obeys (V1) – (V8) if V does. It should also be clear that an equivalent way to define a subspace is to require that $cx + y \in W$ for all $x, y \in W$ and all $c \in \mathcal{F}$.

If W is a subspace of V and $W \neq V$, then W is called a **proper** subspace of V. In particular, $W = \{0\}$ is a subspace of V, but it is not very interesting, and hence from now on we assume that any proper subspace contains more than simply the zero vector. (One sometimes refers to $\{0\}$ and V as **trivial** subspaces of V.)

Example 2.4 Consider the elementary Euclidean space $\mathbb{R}^3$ consisting of all triples (x, y, z) of scalars. If we restrict our consideration to those vectors of the form (x, y, 0), then we obtain a subspace of $\mathbb{R}^3$. In fact, this subspace is essentially just the space $\mathbb{R}^2$ which we think of as the usual xy-plane. We leave it as a simple exercise for the reader to show that this does indeed define a subspace of $\mathbb{R}^3$. Note that any other plane parallel to the xy–plane is *not* a subspace. ∕∕

Example 2.5 Let V be a vector space over $\mathcal{F}$, and let $S = \{x_1, \ldots, x_n\}$ be any n vectors in V. Given any set of scalars $\{a_1, \ldots, a_n\}$, the vector

$$\sum_{i=1}^{n} a_i x_i = a_1 x_1 + \cdots + a_n x_n$$

is called a **linear combination** of the n vectors $x_i \in S$, and the set $\mathcal{S}$ of all such linear combinations of elements in S is called the subspace **spanned** (or **generated**) by S. Indeed, if $A = \sum_{i=1}^{n} a_i x_i$ and $B = \sum_{i=1}^{n} b_i x_i$ are vectors in $\mathcal{S}$ and $c \in \mathcal{F}$, then both

$$A + B = \sum_{i=1}^{n} (a_i + b_i) x_i$$

and

$$cA = \sum_{i=1}^{n} (ca_i) x_i$$

are vectors in $\mathcal{S}$. Hence $\mathcal{S}$ is a subspace of V. $\mathcal{S}$ is sometimes called the **linear span** of S, and we say that S **spans** $\mathcal{S}$. ∕∕

In view of this example, we might ask whether or not *every* vector space is in fact the linear span of some set of vectors in the space. In the next section we shall show that this leads naturally to the concept of the dimension of a vector space.

Exercises

1. Verify axioms (V1) – (V8) for the space $\mathcal{F}^n$.

2. Let S be any set, and consider the collection V of all mappings f of S into a field $\mathcal{F}$. For any f, g ∈ V and $\alpha \in \mathcal{F}$, we define $(f + g)(x) = f(x) + g(x)$ and $(\alpha f)(x) = \alpha f(x)$ for every x ∈ S. Show that V together with these operations defines a vector space over $\mathcal{F}$.

3. Consider the two element set {x, y} with addition and scalar multiplication by $c \in \mathcal{F}$ defined by

   $$x + x = x \qquad x + y = y + x = y \qquad y + y = x \qquad cx = x \qquad cy = x.$$

   Does this define a vector space over $\mathcal{F}$?

4. Let V be a vector space over $\mathcal{F}$. Show that if x ∈ V and $a, b \in \mathcal{F}$ with $a \neq b$, then $ax = bx$ implies that $x = 0$.

5. Let (V, +, •) be a real vector space with the addition operation denoted by + and the scalar multiplication operation denoted by •. Let $v_0 \in V$ be fixed. We define a new addition operation ⊕ by $x \oplus y = x + y + v_0$, and a new scalar multiplication operation ⊗ by $\alpha \otimes x = \alpha \bullet x + (\alpha - 1) \bullet v_0$. Show that (V, ⊕ , ⊗) defines a real vector space.

6. Let F[ℝ] denote the space of all real-valued functions defined on ℝ with addition and scalar multiplication defined as in Exercise 1.2. In other words, f ∈ F[ℝ] means $f: \mathbb{R} \rightarrow \mathbb{R}$.
   (a) Let C[ℝ] denote the set of all continuous real-valued functions defined on ℝ. Show that C[ℝ] is a subspace of F[ℝ].
   (b) Repeat part (a) with the set D[ℝ] of all such differentiable functions.

7. Referring to the previous exercise, let $D^n[\mathbb{R}]$ denote the set of all n-times differentiable functions from ℝ to ℝ. Consider the subset V of $D^n[\mathbb{R}]$ given by the set of all functions that satisfy the differential equation

$$f^{(n)}(x) + a_{n-1}f^{(n-1)}(x) + a_{n-2}f^{(n-2)}(x) + \cdots + a_1 f^{(1)}(x) + a_0 f(x) = 0$$

where $f^{(i)}(x)$ denotes the i*th* derivative of f(x) and a_i is a fixed real constant. Show that V is a vector space.

8. Let V = $\mathbb{R}^3$. In each of the following cases, determine whether or not the subset W is a subspace of V:
(a) W = {(x, y, 0): x, y ∈ $\mathbb{R}$} (see Example 2.4).
(b) W = {(x, y, z) ∈ $\mathbb{R}^3$: z ≥ 0}.
(c) W = {(x, y, z) ∈ $\mathbb{R}^3$: $x^2 + y^2 + z^2 \le 1$}.
(d) W = {(x, y, z) ∈ $\mathbb{R}^3$: x + y + z = 0}.
(e) W = {(x, y, z) ∈ $\mathbb{R}^3$: x, y, z ∈ $\mathbb{Q}$}.
(f) W = {(x, y, z) ∈ $\mathbb{R}^3$ − {0, 0, 0}}.

9. Let S be a nonempty subset of a vector space V. In Example 2.5 we showed that the linear span $\mathcal{S}$ of S is a subspace of V. Show that if W is any other subspace of V containing S, then $\mathcal{S} \subset$ W.

10. (a) Determine whether or not the intersection $\cap_{i=1}^{n} W_i$ of a finite number of subspaces W_i of a vector space V is a subspace of V.
(b) Determine whether or not the union $\cup_{i=1}^{n} W_i$ of a finite number of subspaces W_i of a space V is a subspace of V.

11. Let W_1 and W_2 be subspaces of a space V such that $W_1 \cup W_2$ is also a subspace of V. Show that one of the W_i is subset of the other.

12. Let W_1 and W_2 be subspaces of a vector space V. If for every v ∈ V we have $v = w_1 + w_2$ where $w_i \in W_i$, then we write $V = W_1 + W_2$ and say that V is the **sum** of the subspaces W_i. If $V = W_1 + W_2$ and $W_1 \cap W_2 = \{0\}$, show that every v ∈ V has a *unique* representation $v = w_1 + w_2$ with $w_i \in W_i$.

13. Let V be the set of all (infinite) real sequences. In other words, any v ∈ V is of the form $(x_1, x_2, x_3, \ldots)$ where each $x_i \in \mathbb{R}$. If we define the addition and scalar multiplication of distinct sequences componentwise exactly as in Example 2.1, then it should be clear that V is a vector space over $\mathbb{R}$. Determine whether or not each of the following subsets of V in fact forms a subspace of V:
(a) All sequences containing only a finite number of nonzero terms.

(b) All sequences of the form $\{x_1, x_2, \dots, x_N, 0, 0, \dots\}$ where N is fixed.

(c) All **decreasing sequences**, i.e., sequences where $x_{k+1} \le x_k$ for each $k = 1, 2, \dots$.

(d) All convergent sequences, i.e., sequences for which $\lim_{k\to\infty} x_k$ exists.

14. For which value of k will the vector $v = (1, -2, k) \in \mathbb{R}^3$ be a linear combination of the vectors $x_1 = (3, 0, -2)$ and $x_2 = (2, -1, -5)$?

15. Write the vector $v = (1, -2, 5)$ as a linear combination of the vectors $x_1 = (1, 1, 1)$, $x_2 = (1, 2, 3)$ and $x_3 = (2, -1, 1)$.

2.2 LINEAR INDEPENDENCE AND BASES

Let $x_1, \dots, x_n$ be vectors in a vector space V. We say that these vectors are **linearly dependent** if there exist scalars $a_1, \dots, a_n \in \mathcal{F}$, not all equal to 0, such that

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = \sum_{i=1}^{n} a_ix_i = 0.$$

The vectors x_i are said to be **linearly independent** if they are not linearly dependent. From these definitions, it follows that any set containing a linearly dependent subset must be linearly dependent, and any subset of a linearly independent set is necessarily linearly independent.

It is important to realize that a set of vectors may be linearly dependent with respect to one field, but independent with respect to another. For example, the set $\mathbb{C}$ of all complex numbers is itself a vector space over either the field of real numbers or over the field of complex numbers. However, the set $\{x_1 = 1, x_2 = i\}$ is linearly independent if $\mathcal{F} = \mathbb{R}$, but linearly dependent if $\mathcal{F} = \mathbb{C}$ since $ix_1 + (-1)x_2 = 0$. We will always assume that a linear combination is taken with respect to the same field that V is defined over.

As a means of simplifying our notation, we will frequently leave off the limits of a sum when there is no possibility of ambiguity. Thus, if we are considering the set $\{x_1, \dots, x_n\}$, then a linear combination of the x_i will often be written as $\sum a_ix_i$ rather than $\sum_{i=1}^{n} a_ix_i$. In addition, we will often denote a collection $\{x_1, \dots, x_n\}$ of vectors simply by $\{x_i\}$.

Example 2.6 Consider the three vectors in $\mathbb{R}^3$ given by

$$e_1 = (1, 0, 0)$$
$$e_2 = (0, 1, 0)$$
$$e_3 = (0, 0, 1).$$

Using the definitions of addition and scalar multiplication given in Example 2.1, it is easy to see that these three vectors are linearly independent. This is because the zero vector in $\mathbb{R}^3$ is given by (0, 0, 0), and hence

$$a_1 e_1 + a_2 e_2 + a_3 e_3 = (a_1, a_2, a_3) = (0, 0, 0)$$

implies that $a_1 = a_2 = a_3 = 0$.

On the other hand, the vectors

$$x_1 = (1, 0, 0)$$
$$x_2 = (0, 1, 2)$$
$$x_3 = (1, 3, 6)$$

are linearly dependent since $x_3 = x_1 + 3x_2$. //

Theorem 2.2 A finite set S of vectors in a space V is linearly dependent if and only if one vector in the set is a linear combination of the others. In other words, S is linearly dependent if one vector in S is in the subspace spanned by the remaining vectors in S.

Proof If $S = \{x_1, \dots, x_n\}$ is a linearly dependent subset of V, then

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$$

for some set of scalars $a_1, \dots, a_n \in \mathcal{F}$ not all equal to 0. Suppose, to be specific, that $a_1 \neq 0$. Then we may write

$$x_1 = -(a_2/a_1)x_2 - \cdots - (a_n/a_1)x_n$$

which shows that x_1 is a linear combination of $x_2, \dots, x_n$.

Conversely, if $x_1 = \Sigma_{i\neq 1} a_i x_i$ then

$$x_1 + (-a_2)x_2 + \cdots + (-a_n)x_n = 0$$

which shows that the collection $\{x_1, \dots, x_n\}$ is linearly dependent. ∎

It is important to realize that no linearly independent set of vectors can contain the zero vector. To see this, note that if $S = \{x_1, \dots, x_n\}$ and $x_1 = 0$, then $ax_1 + 0x_2 + \cdots + 0x_n = 0$ for all $a \in \mathcal{F}$, and hence by definition, S is a linearly dependent set.

Theorem 2.3 Let $S = \{x_1, \dots, x_n\} \subset V$ be a linearly independent set, and let $\mathcal{S}$ be the linear span of S. Then every $v \in \mathcal{S}$ has a unique representation

$$v = \sum_{i=1}^{n} a_i x_i$$

where each $a_i \in \mathcal{F}$.

Proof By definition of $\mathcal{S}$, we can always write $v = \Sigma a_i x_i$. As to uniqueness, it must be shown that if we also have $v = \Sigma b_i x_i$, then it follows that $b_i = a_i$ for every $i = 1, \dots, n$. But this is easy since $\Sigma a_i x_i = \Sigma b_i x_i$ implies $\Sigma(a_i - b_i)x_i = 0$, and hence $a_i - b_i = 0$ (since $\{x_i\}$ is linearly independent). Therefore $a_i = b_i$ for each $i = 1, \dots, n$. ∎

If S is a finite subset of a vector space V such that $V = \mathcal{S}$ (the linear span of S), then we say that V is **finite-dimensional**. However, we must define what is meant in general by the dimension of V. If $S \subset V$ is a linearly independent set of vectors with the property that $V = \mathcal{S}$, then we say that S is a **basis** for V. In other words, a **basis** for V is a linearly independent set that spans V. We shall see that the number of elements in a basis is what is meant by the **dimension** of V. But before we can state this precisely, we must be sure that such a number is well-defined. In other words, we must show that any basis has the same number of elements. We prove this (see the corollary to Theorem 2.6) in several steps.

Theorem 2.4 Let $\mathcal{S}$ be the linear span of $S = \{x_1, \dots, x_n\} \subset V$. If $k \le n$ and $\{x_1, \dots, x_k\}$ is linearly independent, then there exists a linearly independent subset of S of the form $\{x_1, \dots, x_k, x_{i_1}, \dots, x_{i_\alpha}\}$ whose linear span also equals $\mathcal{S}$.

Proof If $k = n$ there is nothing left to prove, so we assume that $k < n$. Since $x_1, \dots, x_k$ are linearly independent, we let x_j (where $j > k$) be the first vector in S that is a linear combination of the preceding $x_1, \dots, x_{j-1}$. If no such j exists, then take $(i_1, \dots, i_\alpha) = (k + 1, \dots, n)$. Then the set of $n - 1$ vectors $x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n$ has a linear span that must be contained in $\mathcal{S}$ (since this set is just a subset of S). However, if v is any vector in $\mathcal{S}$, we can write $v = \sum_{i=1}^{n} a_i x_i$ where x_j is just a linear combination of the first $j - 1$ vectors. In other words, v is a linear combination of $x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n$ and hence these n - 1 vectors also span $\mathcal{S}$.

We now continue this process by picking out the first vector in this set of n - 1 vectors that is a linear combination of the preceding vectors. An identical argument shows that the linear span of this set of n - 2 vectors must also be $\mathcal{S}$. It is clear that we will eventually obtain a set $\{x_1, \dots, x_k, x_{i_1}, \dots, x_{i_\alpha}\}$ whose linear span is still $\mathcal{S}$, but in which no vector is a linear combination of the preceding ones. This means that the set must be linearly independent (Theorem 2.2). ∎

Corollary 1 If V is a finite-dimensional vector space such that the set $S = \{x_1, \dots, x_m\} \subset V$ spans V, then some subset of S is a basis for V.

Proof By Theorem 2.4, S contains a linearly independent subset that also spans V. But this is precisely the requirement that S contain a basis for V. ∎

Corollary 2 Let V be a finite-dimensional vector space and let $\{x_1, \dots, x_n\}$ be a basis for V. Then any element $v \in V$ has a unique representation of the form

$$v = \sum_{i=1}^{n} a_i x_i$$

where each $a_i \in \mathcal{F}$.

Proof Since $\{x_i\}$ is linearly independent and spans V, Theorem 2.3 shows us that any $v \in V$ may be written in the form $v = \sum_{i=1}^{n} a_i x_i$ where each $a_i \in \mathcal{F}$ is unique (for this particular basis). ∎

It is important to realize that Corollary 1 asserts the existence of a finite basis in any finite-dimensional vector space, but says nothing about the uniqueness of this basis. In fact, there are an infinite number of possible bases for any such space. However, by Corollary 2, once a particular basis has been chosen, then any vector has a unique expansion in terms of this basis.

Example 2.7 Returning to the space $\mathcal{F}^n$, we see that any $(a_1, \dots, a_n) \in \mathcal{F}^n$ can be written as the linear combination

$$a_1(1, 0, \dots, 0) + a_2(0, 1, 0, \dots, 0) + \cdots + a_n(0, \dots, 0, 1) \; .$$

This means that the n vectors

$$\begin{aligned} e_1 &= (1, 0, 0, \dots, 0) \\ e_2 &= (0, 1, 0, \dots, 0) \\ &\vdots \\ e_n &= (0, 0, 0, \dots, 1) \end{aligned}$$

span $\mathcal{F}^n$. They are also linearly independent since $\sum a_i e_i = (a_1, \dots, a_n) = 0$ if and only if $a_i = 0$ for all $i = 1, \dots, n$. The set $\{e_i\}$ is extremely useful, and will be referred to as the **standard basis** for $\mathcal{F}^n$. //

This example leads us to make the following generalization. By an **ordered basis** for a finite-dimensional space V, we mean a finite sequence of vectors that is linearly independent and spans V. If the sequence $x_1, \dots, x_n$ is an ordered basis for V, then the set $\{x_1, \dots, x_n\}$ is a basis for V. In other words, the set $\{x_1, \dots, x_n\}$ gives rise to n! different ordered bases. Since there is usually nothing lost in assuming that a basis is ordered, we shall continue to assume that $\{x_1, \dots, x_n\}$ denotes an ordered basis unless otherwise noted.

Given any (ordered) basis $\{x_1, \dots, x_n\}$ for V, we know that any $v \in V$ has a unique representation $v = \sum_{i=1}^n a_i x_i$. We call the scalars $a_1, \dots, a_n$ the **coordinates** of v relative to the (ordered) basis $\{x_1, \dots, x_n\}$. In particular, we call a_i the *ith* coordinate of v. Moreover, we now proceed to show that these coordinates define an isomorphism between V and $\mathcal{F}^n$.

Since a vector space is also an (additive abelian) group, it is reasonable that we make the following definition. Let V and W be vector spaces over $\mathcal{F}$. We say that a mapping $\phi: V \rightarrow W$ is a **vector space homomorphism** (or, as we shall call it later, a **linear transformation**) if

$$\phi(x + y) = \phi(x) + \phi(y)$$

and

$$\phi(ax) = a\phi(x)$$

for all $x, y \in V$ and $a \in \mathcal{F}$. This agrees with our previous definition for groups, except that now we must take into account the multiplication by scalars. If ϕ is injective, then we say that ϕ is an **isomorphism**, and if ϕ is bijective, that V and W are **isomorphic**.

As before, we define the kernel of ϕ to be the set

$$\text{Ker}\,\phi = \{x \in V: \phi(x) = 0 \in W\} .$$

If $x, y \in \text{Ker}\,\phi$ and $c \in F$ we have

$$\phi(x + y) = \phi(x) + \phi(y) = 0$$

and

$$\phi(cx) = c\phi(x) = c0 = 0 .$$

This shows that both x + y and cx are in Ker ϕ, and hence Ker ϕ is a subspace of V. Note also that if a = 0 and x ∈ V then

$$\phi(0) = \phi(ax) = a\phi(x) = 0 .$$

Alternatively, we could also note that

$$\phi(x) = \phi(x + 0) = \phi(x) + \phi(0)$$

and hence ϕ(0) = 0. Finally, we see that

$$0 = \phi(0) = \phi(x + (-x)) = \phi(x) + \phi(-x)$$

and therefore

$$\phi(-x) = -\phi(x) .$$

Our next result is essentially the content of Theorem 1.6 and its corollary.

Theorem 2.5 Let ϕ: V → W be a vector space homomorphism. Then ϕ is an isomorphism if and only if Ker ϕ = {0}.

Proof If ϕ is injective, then the fact that ϕ(0) = 0 implies that we must have Ker ϕ = {0}. Conversely, if Ker ϕ = {0} and ϕ(x) = ϕ(y), then

$$0 = \phi(x) - \phi(y) = \phi(x - y)$$

implies that x - y = 0, or x = y. ∎

Now let us return to the above notion of an ordered basis. For any finite-dimensional vector space V over $\mathcal{F}$ and any (ordered) basis $\{x_1, \ldots, x_n\}$, we define a mapping $\phi\colon V \to \mathcal{F}^n$ by

$$\phi(v) = \phi\left(\sum_{i=1}^{n} a_i x_i\right) = (a_1, \ldots, a_n)$$

for each

$$v = \sum_{i=1}^{n} a_i x_i \in V.$$

Since

$$\begin{aligned}\phi(\Sigma a_i x_i + \Sigma b_i x_i) &= \phi(\Sigma(a_i + b_i)x_i)\\ &= (a_1 + b_1, \dots, a_n + b_n)\\ &= (a_1, \dots, a_n) + (b_1, \dots, b_n)\\ &= \phi(\Sigma a_i x_i) + \phi(\Sigma b_i x_i)\end{aligned}$$

and

$$\begin{aligned}\phi(kv) &= \phi(k\Sigma a_i x_i) = \phi(\Sigma(ka_i)x_i) = (ka_1, \dots, ka_n) = k(a_1, \dots, a_n)\\ &= k\phi(v)\end{aligned}$$

we see that ϕ is a vector space homomorphism. Because the coordinates of any vector are unique for a fixed basis, we see that this mapping is indeed well-defined and one-to-one. (Alternatively, the identity element in the space $\mathcal{F}^n$ is $(0, \dots, 0)$, and the only vector that maps into this is the zero vector in V. Hence Ker $\phi = \{0\}$ and ϕ is an isomorphism.) It is clear that ϕ is surjective since, given any ordered set of scalars $a_1, \dots, a_n \in \mathcal{F}$, we can define the vector $v = \Sigma a_i x_i \in V$. Therefore we have shown that V and $\mathcal{F}^n$ are isomorphic for some n, where n is the number of vectors in an ordered basis for V.

If V has a basis consisting of n elements, is it possible to find another basis consisting of $m \neq n$ elements? Intuitively we guess not, for if this were true then V would be isomorphic to $\mathcal{F}^m$ as well as to $\mathcal{F}^n$, which implies that $\mathcal{F}^m$ is isomorphic to $\mathcal{F}^n$ for $m \neq n$. That this is not possible should be obvious by simply considering the projection of a point in $\mathbb{R}^3$ down onto the plane $\mathbb{R}^2$. Any point in $\mathbb{R}^2$ is thus the image of an entire vertical line in $\mathbb{R}^3$, and hence this projection can not possibly be an isomorphism. Nevertheless, we proceed to prove this in detail beginning with our next theorem.

Theorem 2.6 Let $\{x_1, \dots, x_n\}$ be a basis for V, and let $\{y_1, \dots, y_m\}$ be linearly independent vectors in V. Then $m \leq n$.

Proof Since $\{x_1, \dots, x_n\}$ spans V, we may write each y_i as a linear combination of the x_j. In particular, choosing y_m, it follows that the set

$$\{y_m, x_1, \dots, x_n\}$$

is linearly dependent (Theorem 2.2) and spans V (since the x_k already do so). Hence there must be a proper subset $\{y_m, x_{i_1}, \dots, x_{i_r}\}$ with $r \leq n - 1$ that forms a basis for V (Theorem 2.4). Now this set spans V so that y_{m-1} is a linear combination of this set, and hence

$$\{y_{m-1}, y_m, x_{i_1}, \dots, x_{i_r}\}$$

is linearly dependent and spans V. By Theorem 2.4 again, we can find a set $\{y_{m-1}, y_m, x_{j_1}, \dots, x_{j_s}\}$ with $s \le n - 2$ that is also a basis for V. Continuing our process, we eventually obtain the set

$$\{y_2, \dots, y_m, x_\alpha, x_\beta, \dots\}$$

which spans V and must contain at least one of the x_k (since y_1 is not a linear combination of the set $\{y_2, \dots, y_m\}$ by hypothesis). This set was constructed by adding $m - 1$ vectors y_i to the original set of n vectors x_k, and deleting at least $m - 1$ of the x_k along the way. However, we still have at least one of the x_k in our set, and hence it follows that $m - 1 \le n - 1$ or $m \le n$. ∎

Corollary Any two bases for a finite-dimensional vector space must consist of the same number of elements.

Proof Let $\{x_1, \dots, x_n\}$ and $\{y_1, \dots, y_m\}$ be bases for V. Since the y_i are linearly independent, Theorem 2.6 says that $m \le n$. On the other hand, the x_j are linearly independent so that $n \le m$. Therefore we must have $n = m$. ∎

We now return to the proof that $\mathcal{F}^m$ is isomorphic to $\mathcal{F}^n$ if and only if $m = n$. Let us first show that an isomorphism maps a basis to a basis.

Theorem 2.7 Let $\phi: V \to W$ be an isomorphism of finite-dimensional vector spaces. Then a set of vectors $\{\phi(v_1), \dots, \phi(v_n)\}$ is linearly dependent in W if and only if the set $\{v_1, \dots, v_n\}$ is linearly dependent in V.

Proof If the set $\{v_1, \dots, v_n\}$ is linearly dependent, then for some set of scalars $\{a_1, \dots, a_n\}$ not all equal to 0 we have $\sum_{i=1}^n a_i v_i = 0$. Applying ϕ to both sides of this equation yields

$$0 = \phi(0) = \phi(\Sigma a_i v_i) = \Sigma \phi(a_i v_i) = \Sigma a_i \phi(v_i) .$$

But since not all of the a_i are 0, this means that $\{\phi(v_i)\}$ must be linearly dependent.

Conversely, if $\phi(v_1), \dots, \phi(v_n)$ are linearly dependent, then there exists a set of scalars $b_1, \dots, b_n$ not all 0 such that $\Sigma b_i \phi(v_i) = 0$. But this means

$$0 = \Sigma b_i \phi(v_i) = \Sigma \phi(b_i v_i) = \phi(\Sigma b_i v_i)$$

which implies that $\sum b_i v_i = 0$ (since Ker $\phi = \{0\}$). This shows that the set $\{v_i\}$ is linearly dependent. ∎

Corollary If $\phi\colon V \rightarrow W$ is an isomorphism of finite-dimensional vector spaces, then $\{\phi(x_i)\} = \{\phi(x_1), \dots, \phi(x_n)\}$ is a basis for W if and only if $\{x_i\} = \{x_1, \dots, x_n\}$ is a basis for V.

Proof Since ϕ is an isomorphism, for any vector $w \in W$ there exists a unique $v \in V$ such that $\phi(v) = w$. If $\{x_i\}$ is a basis for V, then $v = \sum_{i=1}^{n} a_i x_i$ and

$$w = \phi(v) = \phi(\sum a_i x_i) = \sum a_i \phi(x_i) \ .$$

Hence the $\phi(x_i)$ span W, and they are linearly independent by Theorem 2.7.

On the other hand, if $\{\phi(x_i)\}$ is a basis for W, then there exist scalars $\{b_i\}$ such that for any $v \in V$ we have

$$\phi(v) = w = \sum b_i \phi(x_i) = \phi(\sum b_i x_i) \ .$$

Since ϕ is an isomorphism, this implies that $v = \sum b_i x_i$, and hence $\{x_i\}$ spans V. The fact that it is linearly independent follows from Theorem 2.7. This shows that $\{x_i\}$ is a basis for V. ∎

Theorem 2.8 $\mathcal{F}^n$ is isomorphic to $\mathcal{F}^m$ if and only if n = m.

Proof If n = m the result is obvious. Now assume that $\mathcal{F}^n$ and $\mathcal{F}^m$ are isomorphic. We have seen in Example 2.7 that the standard basis of $\mathcal{F}^n$ consists of n vectors. Since an isomorphism carries one basis onto another (corollary to Theorem 2.7), any space isomorphic to $\mathcal{F}^n$ must have a basis consisting of n vectors. Hence by the corollary to Theorem 2.6 we must have m = n. ∎

Corollary If V is a finite-dimensional vector space over $\mathcal{F}$, then V is isomorphic to $\mathcal{F}^n$ for a unique integer n.

Proof It was shown following Theorem 2.5 that V is isomorphic to $\mathcal{F}^n$ for some integer n, and Theorem 2.8 shows that n must be unique. ∎

The corollary to Theorem 2.6 shows us that the number of elements in any basis for a finite-dimensional vector space is fixed. We call this unique number n the **dimension** of V over $\mathcal{F}$, and we write dim V = n. Our next result agrees with our intuition, and is quite useful in proving other theorems.

Theorem 2.9 Every subspace W of a finite-dimensional vector space V is finite-dimensional, and dim W ≤ dim V.

Proof We must show that W has a basis, and that this basis contains at most n = dim V elements. If W = {0}, then dim W = 0 ≤ n and we are done. If W contains some $x_1 \neq 0$, then let $W_1 \subset W$ be the subspace spanned by x_1. If W = W_1, then dim W = 1 and we are done. If W ≠ W_1, then there exists some $x_2 \in$ W with $x_2 \notin W_1$, and we let W_2 be the subspace spanned by $\{x_1, x_2\}$. Again, if W = W_2, then dim W = 2. If W ≠ W_2, then choose some $x_3 \in$ W with $x_3 \notin W_2$ and continue this procedure. However, by Theorem 2.6, there can be at most n linearly independent vectors in V, and hence dim W ≤ n. ∎

Note that the zero subspace is spanned by the vector 0, but {0} is not linearly independent so it can not form a basis. Therefore the zero subspace is *defined* to have dimension zero.

Finally, let us show that any set of linearly independent vectors may be extended to form a complete basis.

Theorem 2.10 Let V be finite-dimensional and S = $\{x_1, \dots, x_m\}$ any set of m linearly independent vectors in V. Then there exists a set $\{x_{m+1}, \dots, x_{m+r}\}$ of vectors in V such that $\{x_1, \dots, x_{m+r}\}$ is a basis for V.

Proof Since V is finite-dimensional, it has a basis $\{v_1, \dots, v_n\}$. Then the set $\{x_1, \dots, x_m, v_1, \dots, v_n\}$ spans V so, by Theorem 2.4, we can choose a subset $\{x_1, \dots, x_m, v_{i_1}, \dots, v_{i_r}\}$ of linearly independent vectors that span V. Letting $v_{i_1} = x_{m+1}, \dots, v_{i_r} = x_{m+r}$ proves the theorem. ∎

Exercises

1. Determine whether or not the three vectors $x_1 = (2, -1, 0)$, $x_2 = (1, -1, 1)$ and $x_3 = (0, 2, 3)$ form a basis for $\mathbb{R}^3$.

2. In each of the following, show that the given set of vectors is linearly independent, and decide whether or not it forms a basis for the indicated space:
   (a) $\{(1, 1), (1, -1)\}$ in $\mathbb{R}^2$.
   (b) $\{(2, 0, 1), (1, 2, 0), (0, 1, 0)\}$ in $\mathbb{R}^3$.
   (c) $\{(1, 0, 0, 0), (1, 1, 0, 0), (1, 1, 1, 0), (1, 1, 1, 1)\}$ in $\mathbb{R}^4$.

3. Extend each of the following sets to a basis for the given space:
(a) $\{(1, 1, 0), (2, -2, 0)\}$ in $\mathbb{R}^3$.
(b) $\{(1, 0, 0, 0), (1, 0, 1, 0), (1, 0, 0, 1)\}$ in $\mathbb{R}^4$.
(c) $\{(1, 1, 0, 0), (1, -1, 0, 0), (1, 0, 1, 0)\}$ in $\mathbb{R}^4$.

4. Show that the vectors $u = (1 + i, 2i)$, $v = (1, 1 + i) \in \mathbb{C}^2$ are linearly dependent over $\mathbb{C}$, but linearly independent over $\mathbb{R}$.

5. Find the coordinates of the vector $(3, 1, -4) \in \mathbb{R}^3$ relative to the basis $x_1 = (1, 1, 1)$, $x_2 = (0, 1, 1)$ and $x_3 = (0, 0, 1)$.

6. Let $\mathbb{R}_3[x]$ be the space of all real polynomials of degree ≤ 3. Determine whether or not each of the following sets of polynomials is linearly independent:
(a) $\{x^3 - 3x^2 + 5x + 1, x^3 - x^2 + 8x + 2, 2x^3 - 4x^2 + 9x + 5\}$.
(b) $\{x^3 + 4x^2 - 2x + 3, x^3 + 6x^2 - x + 4, 3x^3 + 8x^2 - 8x + 7\}$.

7. Let V be a finite-dimensional space, and let W be any subspace of V. Show that there exists a subspace W′ of V such that $W \cap W' = \{0\}$ and $V = W + W'$ (see Exercise 1.12 for the definition of W + W′).

8. Let $\phi: V \rightarrow W$ be a homomorphism of two vector spaces V and W.
(a) Show that ϕ maps any subspace of V onto a subspace of W.
(b) Let S′ be a subspace of W, and define the set $S = \{x \in V: \phi(x) \in S'\}$. Show that S is a subspace of V.

9. Let V be finite-dimensional, and assume that $\phi: V \rightarrow V$ is a surjective homomorphism. Prove that ϕ is in fact an isomorphism of V onto V.

10. Let V have basis $x_1, x_2, \ldots, x_n$, and let $v_1, v_2, \ldots, v_n$ be any n elements in V. Define a mapping $\phi: V \rightarrow V$ by

$$\phi\left(\sum_{i=1}^{n} a_i x_i\right) = \sum_{i=1}^{n} a_i v_i$$

where each $a_i \in \mathcal{F}$.
(a) Show that ϕ is a surjective homomorphism.
(b) When is ϕ an isomorphism?

2.3 DIRECT SUMS

We now present some useful ways of constructing a new vector space from several given spaces. The reader is advised to think carefully about these concepts, as they will become quite important later in this book. We also repeat our earlier remark that all of the vector spaces that we are discussing are considered to be defined over the same field $\mathcal{F}$.

Let A and B be subspaces of a finite-dimensional vector space V. Then we may define the **sum** of A and B to be the set A + B given by

$$A + B = \{a + b: a \in A \text{ and } b \in B\} .$$

It is important to note that A and B must both be subspaces of the same space V, or else the addition of $a \in A$ to $b \in B$ is not defined. In fact, since A and B are subspaces of V, it is easy to show that A + B is also subspace of V. Indeed, given any $a_1 + b_1$ and $a_2 + b_2$ in A + B and any $k \in \mathcal{F}$ we see that

$$(a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2) \in A + B$$

and

$$k(a_1 + b_1) = ka_1 + kb_1 \in A + B$$

as required. This definition can clearly be extended by induction to any finite collection $\{A_i\}$ of subspaces.

In addition to the sum of the subspaces A and B, we may define their **intersection** $A \cap B$ by

$$A \cap B = \{x \in V: x \in A \text{ and } x \in B\} .$$

Since A and B are subspaces, we see that for any $x, y \in A \cap B$ we have both $x + y \in A$ and $x + y \in B$ so that $x + y \in A \cap B$, and if $x \in A \cap B$ then $kx \in A$ and $kx \in B$ so that $kx \in A \cap B$. Since $0 \in A \cap B$, we then see that $A \cap B$ is a nonempty subspace of V. This can also be extended to any finite collection of subspaces of V.

Our next theorem shows that the dimension of the sum of A and B is just the sum of the dimensions of A and B minus the dimension of their intersection.

Theorem 2.11 If A and B are subspaces of a finite-dimensional space V, then

$$\dim(A + B) = \dim A + \dim B - \dim(A \cap B) .$$

Proof Since A + B and A ∩ B are subspaces of V, it follows that both A + B and A ∩ B are finite-dimensional (Theorem 2.9). We thus let dim A = m, dim B = n and dim A ∩ B = r.

Let $\{u_1, \dots, u_r\}$ be a basis for A ∩ B. By Theorem 2.10 there exists a set $\{v_1, \dots, v_{m-r}\}$ of linearly independent vectors in V such that

$$\{u_1, \dots, u_r, v_1, \dots \quad, v_{m-r}\}$$

is a basis for A. Similarly, we have a basis

$$\{u_1, \dots, u_r, w_1, \dots, w_{n-r}\}$$

for B. It is clear that the set

$$\{u_1, \dots, u_r, v_1, \dots, v_{m-r}, w_1, \dots, w_{n-r}\}$$

spans A + B since any a + b ∈ A + B (with a ∈ A and b ∈ B) can be written as a linear combination of these r + (m - r) + (n - r) = m + n - r vectors. To prove that they form a basis for A + B, we need only show that these m + n - r vectors are linearly independent.

Suppose we have sets of scalars $\{a_i\}$, $\{b_j\}$ and $\{c_k\}$ such that

$$\sum_{i=1}^{r} a_i u_i + \sum_{j=1}^{m-r} b_j v_j + \sum_{k=1}^{n-r} c_k w_k = 0$$

Then

$$\sum_{i=1}^{r} a_i u_i + \sum_{j=1}^{m-r} b_j v_j = -\sum_{k=1}^{n-r} c_k w_k .$$

Since the left side of this equation is an element of A while the right side is an element of B, their equality implies that they both belong to A ∩ B, and hence

$$-\sum_{k=1}^{n-r} c_k w_k = \sum_{i=1}^{r} d_i u_i$$

for some set of scalars $\{d_i\}$. But $\{u_1, \dots, u_r, w_1, \dots, w_{n-r}\}$ forms a basis for B and hence they are linearly independent. Therefore, writing the above equation as

$$\sum_{i=1}^{r} d_i u_i + \sum_{k=1}^{n-r} c_k w_k = 0$$

implies that

$$d_1 = \cdots = d_r = c_1 = \cdots = c_{n-r} = 0 .$$

We are now left with

$$\sum_{i=1}^{r} a_i u_i + \sum_{j=1}^{m-r} b_j v_j = 0.$$

But $\{u_1, \ldots, u_r, v_1, \ldots, v_{m-r}\}$ is also linearly independent so that

$$a_1 = \cdots = a_r = b_1 = \cdots = b_{m-r} = 0 \ .$$

This proves that $\{u_1, \ldots, u_r, v_1, \ldots, v_{m-r}, w_1, \ldots, w_{n-r}\}$ is linearly independent as claimed. The proof is completed by simply noting that we have shown

$$\dim(A + B) = m + n - r = \dim A + \dim B - \dim(A \cap B) \ . \ ∎$$

We now consider a particularly important special case of the sum. If A and B are subspaces of V such that $A \cap B = \{0\}$ and $V = A + B$, then we say that V is the **internal direct sum** of A and B. A completely equivalent way of defining the internal direct sum is given in the following theorem.

Theorem 2.12 Let A and B be subspaces of a finite-dimensional vector space V. Then V is the internal direct sum of A and B if and only if every $v \in V$ can be *uniquely* written in the form $v = a + b$ where $a \in A$ and $b \in B$.

Proof Let us first assume that V is the internal direct sum of A and B. In other words, $V = A + B$ and $A \cap B = \{0\}$. Then by definition, for any $v \in V$ we have $v = a + b$ for some $a \in A$ and $b \in B$. Suppose we also have $v = a' + b'$ where $a' \in A$ and $b' \in B$. Then $a + b = a' + b'$ so that $a - a' = b' - b$. But note that $a - a' \in A$ and $b' - b \in B$, and hence the fact that $A \cap B = \{0\}$ implies that $a - a' = b' - b = 0$. Therefore $a = a'$ and $b = b'$ so that the expression for v is unique.

Conversely, suppose that every $v \in V$ may be written uniquely in the form $v = a + b$ with $a \in A$ and $b \in B$. This means that $V = A + B$, and we must still show that $A \cap B = \{0\}$. In particular, if $v \in A \cap B$ we may write $v = v + 0$ with $v \in A$ and $0 \in B$, or alternatively, we may write $v = 0 + v$ with $0 \in A$ and $v \in B$. But we are assuming that the expression for v is unique, and hence we must have $v = 0$ (since the contributions from A and B must be the same in both cases). Thus $A \cap B = \{0\}$ and the sum is direct. ∎

We emphasize that the internal direct sum is defined for two subspaces A and B of a given space V. As we stated above, this is because the addition of two vectors from distinct spaces is not defined. In spite of this, we now proceed to show that it is nevertheless possible to define the sum of two distinct vector spaces.

Let A and B be distinct vector spaces (over the same field $\mathcal{F}$, of course). While the sum of a vector in A and a vector in B makes no sense, we may relate these two spaces by considering the Cartesian product A × B defined as (see Section 0.1)

$$A \times B = \{(a, b): a \in A \text{ and } b \in B\} \ .$$

Using the ordered pairs (a, b), it is now easy to turn A × B into a vector space by making the following definitions (see Example 2.1).

First, we say that two elements (a, b) and (a′, b′) of A × B are equal if and only if $a = a'$ and $b = b'$. Next, we define addition and scalar multiplication in the obvious manner by

$$(a, b) + (a', b') = (a + a', b + b')$$

and

$$k(a, b) = (ka, kb) \ .$$

We leave it as an exercise for the reader to show that with these definitions, the set A × B defines a vector space V over $\mathcal{F}$. This vector space is called the **external direct sum** of the spaces A and B, and is denoted by $A \oplus B$.

While the external direct sum was defined for arbitrary spaces A and B, there is no reason why this definition can not be applied to two subspaces of a larger space V. We now show that in such a case, the internal and external direct sums are isomorphic.

Theorem 2.13 If V is the internal direct sum of A and B, then V is isomorphic to the external direct sum $A \oplus B$.

Proof If V is the internal direct sum of A and B, then any $v \in V$ may be written uniquely in the form $v = a + b$. This uniqueness allows us to define the mapping $\phi: V \rightarrow A \oplus B$ by

$$\phi(v) = \phi(a + b) = (a, b) \ .$$

Since for any $v = a + b$ and $v' = a' + b'$, and for any scalar k we have

$$\phi(v + v') = (a + a', b + b') = (a, b) + (a', b') = \phi(v) + \phi(v')$$

and

$$\phi(kv) = (ka, kb) = k(a, b) = k\phi(v)$$

it follows that ϕ is a vector space homomorphism. It is clear that ϕ is surjective, since for any $(a, b) \in A \oplus B$ we have $\phi(v) = (a, b)$ where $v = a + b \in V$. Finally, if $\phi(v) = (0, 0)$ then we must have $a = b = 0 = v$ and hence Ker ϕ =

$\{0\}$. This shows that ϕ is also injective (Theorem 2.5). In other words, we have shown that V is isomorphic to $A \oplus B$. ∎

Because of this theorem, we shall henceforth refer only to the **direct sum** of A and B, and denote this sum by $A \oplus B$. It follows trivially from Theorem 2.11 that

$$\dim(A \oplus B) = \dim A + \dim B \ .$$

Example 2.8 Consider the ordinary Euclidean three-space $V = \mathbb{R}^3$. Note that any $v \in \mathbb{R}^3$ may be written as

$$(v_1, v_2, v_3) = (v_1, v_2, 0) + (0, 0, v_3)$$

which is just the sum of a vector in the xy-plane and a vector on the z-axis. It should also be clear that the only vector in the intersection of the xy-plane with the z-axis is the zero vector. In other words, defining the space A to be the xy-plane $\mathbb{R}^2$ and the space B to be the z-axis $\mathbb{R}^1$, we see that $V = A \oplus B$ or $\mathbb{R}^3 = \mathbb{R}^2 \oplus \mathbb{R}^1$.

On the other hand, if we try to write $\mathbb{R}^3$ as the direct sum of the xy-plane A with say, the yz-plane B, then the intersection condition is violated since $A \cap B$ is just the entire y-axis. In this case, any vector lying on the y-axis can be specified in terms of its components in either the xy-plane or in the yz-plane. ∕∕

In many of our later applications we shall need to take the direct sum of several vector spaces. While it should be obvious that this follows simply by induction from the above case, we go through the details nevertheless. We say that a vector space V is the **direct sum** of the subspaces $W_1, \dots, W_r$ if the following properties are true:

(a) $W_i \neq \{0\}$ for each $i = 1, \dots, r$;
(b) $W_i \cap (W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_r) = \{0\}$ for $i = 1, \dots, r$;
(c) $V = W_1 + \cdots + W_r$.

If V is the direct sum of the W_i, then we write $V = W_1 \oplus \cdots \oplus W_r$. The generalization of Theorem 2.12 is the following.

Theorem 2.14 If $W_1, \dots, W_r$ are subspaces of V, then

$$V = W_1 \oplus \cdots \oplus W_r$$

if and only if every $v \in V$ has a unique representation of the form

$$v = v_1 + \cdots + v_r$$

where $v_i \in W_i$ for each $i = 1, \dots, r$.

Proof First assume that V is the direct sum of $W_1, \dots, W_r$. Given any $v \in V$, part (c) in the definition of direct sum tells us that we have

$$v = v_1 + \cdots + v_r$$

where $v_i \in W_i$ for each $i = 1, \dots, r$. If we also have another representation

$$v = v'_1 + \cdots + v'_r$$

with $v'_i \in W_i$, then

$$v_1 + \cdots + v_r = v'_1 + \cdots + v'_r$$

so that for any $i = 1, \dots, r$ we have

$$\begin{aligned} v'_i - v_i = (v_1 - v'_1) + \cdots + (v_{i-1} - v'_{i-1}) &+ (v_{i+1} - v'_{i+1}) \\ &+ \cdots + (v_r - v'_r). \end{aligned}$$

Since $v'_i - v_i \in W_i$ and the right hand side of this equation is an element of $W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_r$, we see that part (b) of the definition requires that $v'_i - v_i = 0$, and hence $v'_i = v_i$. This proves the uniqueness of the representation.

Conversely, assume that each $v \in V$ has a unique representation of the form $v = v_1 + \cdots + v_r$ where $v_i \in W_i$ for each $i = 1, \dots, r$. Since part (c) of the definition of direct sum is automatically satisfied, we must show that part (b) is also satisfied. Suppose

$$v_1 \in W_1 \cap (W_2 + \cdots + W_r) .$$

Since

$$v_1 \in W_2 + \cdots + W_r$$

we must also have

$$v_1 = v_2 + \cdots + v_r$$

for some $v_2 \in W_2, \dots, v_r \in W_r$. But then

$$0 = -v_1 + v_2 + \cdots + v_r$$

and

$$0 = 0 + \cdots + 0$$

are two representations of the vector 0, and hence the uniqueness of the representations implies that $v_i = 0$ for each i = 1, . . . , r. In particular, the case i = 1 means that

$$W_1 \cap (W_2 + \cdots + W_r) = \{0\} \;.$$

A similar argument applies to $W_i \cap (W_2 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_r)$ for any i = 1, . . . , r. This proves part (b) in the definition of direct sum. ∎

If $V = W_1 \oplus \cdots \oplus W_r$, then it seems reasonable that we should be able to form a basis for V by adding up the bases of the subspaces W_i . This is indeed the case as we now show.

Theorem 2.15 Let $W_1, \dots , W_r$ be subspaces of V, and for each i = 1, . . . , r let W_i have basis $B_i = \{w_{i1}, \dots , w_{in_i}\}$. Then V is the direct sum of the W_i if and only if the union of bases

$$B = \cup_{i=1}^r B_i = \{w_{11}, \dots , w_{1n_1} , \dots , w_{r1} , \dots , w_{rn_r}\}$$

is a basis for V.

Proof Suppose that B is a basis for V. Then for any $v \in V$ we may write

$$\begin{aligned} v &= (a_{11}w_{11} + \cdots + a_{1n_1}w_{1n_1}) + \cdots + (a_{r1}w_{r1} + \cdots + a_{rn_r}w_{rn_r}) \\ &= w_1 + \cdots + w_r \end{aligned}$$

where

$$w_i = a_{i1}w_{i1} + \cdots + a_{in_i}w_{in_i} \in W_i$$

and $a_{ij} \in \mathcal{F}$. Now let

$$v = w'_1 + \cdots + w'_r$$

be any other expansion of v, where each $w'_i \in W_i$. Using the fact that B_i is a basis for W_i we have

$$w'_i = b_{i1}w_{i1} + \cdots + b_{in_i}w_{in_i}$$

for some set of scalars b_{ij}. This means that we may also write

$$v = (b_{11}w_{11} + \cdots + b_{1n_1} w_{1n_1}) + \cdots + (b_{r1}w_{r1} + \cdots + b_{rn_r} w_{rn_r}) \;.$$

However, since B is a basis for V, we may equate the coefficients of w_{ij} in these two expressions for v to obtain $a_{ij} = b_{ij}$ for all i, j. We have thus proved that the representation of v is unique, and hence Theorem 2.14 tells us that V is the direct sum of the W_i.

Now suppose that V is the direct sum of the W_i. This means that any $v \in V$ may be expressed in the unique form $v = w_1 + \cdots + w_r$ where $w_i \in W_i$ for each I = 1, . . . , r. Given that $B_i = \{w_{i\,1}, \dots, w_{i\,n_i}\}$ is a basis for W_i, we must show that $B = \cup B_i$ is a basis for V. We first note that each $w_i \in W_i$ may be expanded in terms of the members of B_i , and therefore $\cup B_i$ clearly spans V. It remains to show that the elements of B are linearly independent. We first write

$$(c_{11}w_{11} + \cdots + c_{1n_1}w_{1n_1}) + \cdots + (c_{r\,1}\,w_{r\,1} + \cdots + c_{r\,n_r}\,w_{r\,n_r}) = 0$$

and note that

$$c_{i\,1}\,w_{i\,1} + \cdots + c_{in_i}w_{in_i} \in W_i \ .$$

Using the fact that $0 + \cdots + 0 = 0$ (where each $0 \in W_i$) along with the uniqueness of the representation in any direct sum, we see that for each i = 1, . . . , r we must have

$$c_{il}\,w_{il} + \cdots + c_{in_i}\,w_{in_i} = 0 \ .$$

However, since B_i is a basis for W_i, this means that $c_{i\,j} = 0$ for every i and j, and hence the elements of $B = \cup B_i$ are linearly independent. ∎

Corollary If $V = W_1 \oplus \cdots \oplus W_r$, then

$$\dim\ V = \sum_{i=1}^{r} \dim W_i.$$

Proof Obvious from Theorem 2.15. This also follows by induction from Theorem 2.11. ∎

Exercises

1. Let W_1 and W_2 be subspaces of $\mathbb{R}^3$ defined by $W_1 = \{(x, y, z): x = y = z\}$ and $W_2 = \{(x, y, z): x = 0\}$. Show that $\mathbb{R}^3 = W_1 \oplus W_2$.

2. Let W_1 be any subspace of a finite-dimensional space V. Prove that there exists a subspace W_2 of V such that $V = W_1 \oplus W_2$.

3. Let W_1, W_2 and W_3 be subspaces of a vector space V. Show that

$$(W_1 \cap W_2) + (W_1 \cap W_3) \subset W_1 \cap (W_2 + W_3) \ .$$

Give an example in $V = \mathbb{R}^2$ for which equality does not hold.

4. Let $V = F[\mathbb{R}]$ be as in Exercise 2.1.6. Let W_+ and W_- be the subsets of V defined by $W_+ = \{f \in V: f(-x) = f(x)\}$ and $W_- = \{f \in V: f(-x) = -f(x)\}$. In other words, W_+ is the subset of all even functions, and W_- is the subset of all odd functions.
(a) Show that W_+ and W_- are subspaces of V.
(b) Show that $V = W_+ \oplus W_-$.

5. Let W_1 and W_2 be subspaces of a vector space V.
(a) Show that $W_1 \subset W_1 + W_2$ and $W_2 \subset W_1 + W_2$.
(b) Prove that $W_1 + W_2$ is the smallest subspace of V that contains both W_1 and W_2. In other words, if $\mathcal{S}(W_1, W_2)$ denotes the linear span of W_1 and W_2, show that $W_1 + W_2 = \mathcal{S}(W_1, W_2)$. [*Hint*: Show that $W_1 + W_2 \subset \mathcal{S}(W_1, W_2)$ and $\mathcal{S}(W_1, W_2) \subset W_1 + W_2$.]

6. Let V be a finite-dimensional vector space. For any $x \in V$, we define $\mathcal{F}x = \{ax: a \in \mathcal{F}\}$. Prove that $\{x_1, x_2, \dots, x_n\}$ is a basis for V if and only if $V = \mathcal{F}x_1 \oplus \mathcal{F}x_2 \oplus \cdots \oplus \mathcal{F}x_n$.

7. If A and B are vector spaces, show that A + B is the span of $A \cup B$.

2.4 INNER PRODUCT SPACES

Before proceeding with the general theory of inner products, let us briefly review what the reader should already know from more elementary courses. It is assumed that the reader is familiar with vectors in $\mathbb{R}^3$, and we show that for any $\vec{a}, \vec{b} \in \mathbb{R}^3$ the **scalar product** (also called the "**dot product**") $\vec{a} \bullet \vec{b}$ may be written as either

$$\vec{a} \bullet \vec{b} = \sum_{i=1}^{3} a_i b_i$$

where $\{a_i\}$ and $\{b_i\}$ are the coordinates of $\vec{a}$ and $\vec{b}$ relative to the standard basis for $\mathbb{R}^3$ (see Example 2.7), or as

$$\vec{a} \bullet \vec{b} = \|\vec{a}\| \, \|\vec{b}\| \cos \theta$$

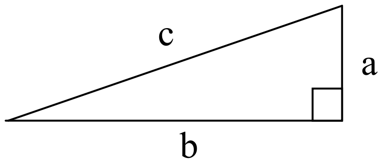
where $\theta = \angle(\vec{a}, \vec{b})$ and

$$\|\vec{a}\|^2 = \sum_{i=1}^{3} a_i{}^2$$

with a similar equation for $\| \vec{b} \|$. The symbol $\|$ is just the vector space generalization of the absolute value of numbers, and will be defined carefully below (see Example 2.9). For now, just think of $\| \vec{a} \|$ as meaning the length of the vector $\vec{a}$ in $\mathbb{R}^3$.

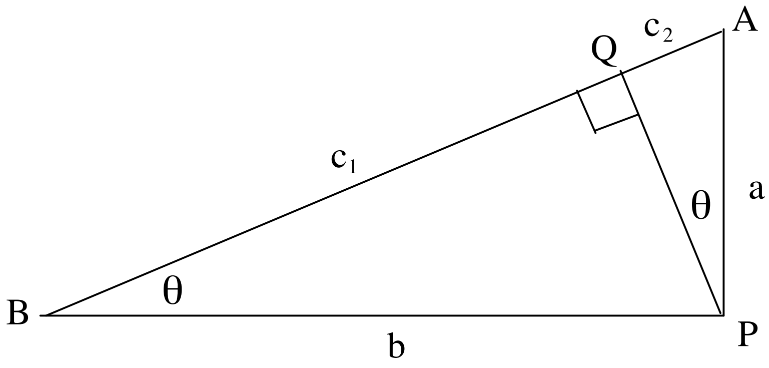
Just for fun, for the sake of completeness, and to show exactly what these equations depend on, we prove this as a series of simple lemmas. Our first lemma is known as the Pythagorean theorem.

Lemma 2.1 Given a right triangle with sides a, b, and c as shown,



we have $c^2 = a^2 + b^2$.

Proof Draw the line PQ perpendicular to the hypotenuse c = AB. Note that we can now write c as the sum of the two parts c_1 and c_2. First observe that the triangle ABP is similar to triangle APQ because they are both right triangles and they have the angle at A in common (so they must have their third angle the same). If we let this third angle be $\theta = \angle(ABP)$, then we also have $\theta = \angle(APQ)$.



Note that the three triangles ABP, APQ and PBQ are all similar, and hence we have (remember $c = c_1 + c_2$)

$$\frac{c_1}{b} = \frac{b}{c} \quad \text{and} \quad \frac{c_2}{a} = \frac{a}{c} \; .$$

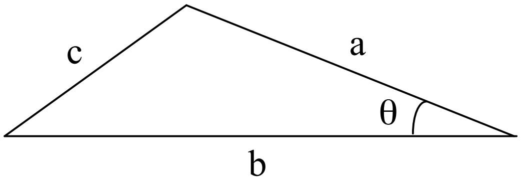
Therefore

$$c = c_1 + c_2 = \frac{a^2 + b^2}{c}$$

from which the lemma follows immediately. ∎

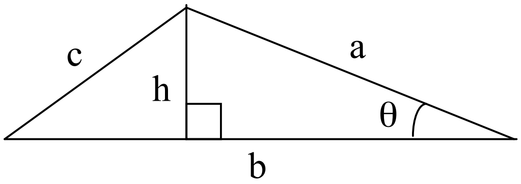
Our next lemma is known as the law of cosines. This law, together with Lemma 2.1, shows that for any triangle T with sides $a \le b \le c$, it is true that $a^2 + b^2 = c^2$ if and only if T is a right triangle.

Lemma 2.2 For any triangle as shown,



we have $c^2 = a^2 + b^2 - 2ab \cos \theta$.

Proof Draw a perpendicular to side b as shown:



By the Pythagorean theorem we have

$$\begin{aligned} c^2 &= h^2 + (b - a\cos\theta)^2 \\ &= (a\sin\theta)^2 + (b - a\cos\theta)^2 \\ &= a^2\sin^2\theta + b^2 - 2ab\cos\theta + a^2\cos^2\theta \\ &= a^2 + b^2 - 2ab\cos\theta \end{aligned}$$

where we used $\sin^2 \theta + \cos^2 \theta = 1$ which follows directly from Lemma 2.1 with $a = c(\sin \theta)$ and $b = c(\cos \theta)$. ∎

We now *define* the scalar product $\vec{a} \bullet \vec{b}$ for any $\vec{a}, \vec{b} \in \mathbb{R}^3$ by

$$\vec{a} \bullet \vec{b} = \sum_{i=1}^{3} a_i b_i = \vec{b} \bullet \vec{a}$$

where $\vec{a} = (a_1, a_2, a_3)$ and $\vec{b} = (b_1, b_2, b_3)$. It is easy to see that

$$\vec{a} \bullet (\vec{b} + \vec{c}) = \sum_{i=1}^{3} a_i(b_i + c_i) = \sum_{i=1}^{3} (a_ib_i + a_ic_i) = \vec{a} \bullet \vec{b} + \vec{a} \bullet \vec{c}$$

and similarly, it is easy to show that

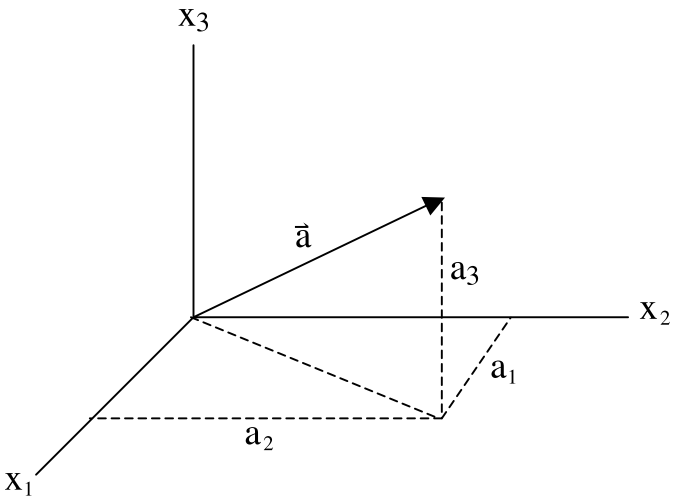
$$(\vec{a} + \vec{b}) \bullet \vec{c} = \vec{a} \bullet \vec{c} + \vec{b} \bullet \vec{c}$$

and

$$(k\vec{a}) \bullet \vec{b} = k(\vec{a} \bullet \vec{b})$$

where $k \in \mathbb{R}$. From the figure below, we see that the Pythagorean theorem also shows us that

$$\| \vec{a} \|^2 = \sum_{i=1}^{3} a_ia_i = \vec{a} \bullet \vec{a} \ .$$



This is the justification for writing $\| \vec{a} \|$ to mean the length of the vector $\vec{a} \in \mathbb{R}^3$.

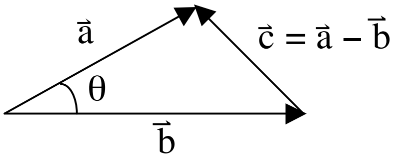
Noting that any two vectors (with a common origin) in $\mathbb{R}^3$ lie in a plane, we have the following well-known formula for the dot product.

Lemma 2.3 For any $\vec{a}, \vec{b} \in \mathbb{R}^3$ we have

$$\vec{a} \bullet \vec{b} = ab \cos \theta$$

where $a = \| \vec{a} \|$, $b = \| \vec{b} \|$ and $\theta = \angle(\vec{a}, \vec{b})$.

Proof Draw the vectors $\vec{a}$ and $\vec{b}$ along with their difference $\vec{c} = \vec{a} - \vec{b}$:



By the law of cosines we have $c^2 = a^2 + b^2 - 2ab \cos \theta$, while on the other hand

$$c^2 = \| \vec{a} - \vec{b} \|^2 = (\vec{a} - \vec{b}) \bullet (\vec{a} - \vec{b}) = a^2 + b^2 - 2\,\vec{a} \bullet \vec{b}\ .$$

Therefore we see that $\vec{a} \bullet \vec{b} = ab \cos \theta$. ∎

The main reason that we went through all of this is to motivate the generalization to arbitrary vector spaces. For example, if $u, v \in \mathbb{R}^n$, then to say that

$$u \bullet v = \sum_{i=1}^{n} u_i v_i$$

makes sense, whereas to say that $u \bullet v = \| u \| \, \| v \| \cos \theta$ leaves one wondering just what the "angle" θ means in higher dimensions. In fact, this will be used to *define* the angle θ.

We now proceed to define a general scalar (or inner) product $\langle u, v\rangle$ of vectors $u, v \in V$. Throughout this section, we let V be a vector space over either the real field $\mathbb{R}$ or the complex field $\mathbb{C}$. By way of motivation, we will want the inner product $\langle\ ,\ \rangle$ applied to a single vector $v \in V$ to yield the length (or norm) of v, so that $\|v\|^2 = \langle v, v\rangle$. But $\|v\|$ must be a real number even if the field we are working with is $\mathbb{C}$. Noting that for any complex number $z \in \mathbb{C}$ we have $|z|^2 = zz^*$, we are led to make the following definition.

Let V be a vector space over $\mathcal{F}$ (where $\mathcal{F}$ is either $\mathbb{R}$ or $\mathbb{C}$). By an **inner product** on V (sometimes called the **Hermitian inner product**), we mean a mapping $\langle\ ,\ \rangle\colon V \times V \to \mathcal{F}$ such that for all $u, v, w \in V$ and $a, b \in \mathcal{F}$ we have

(IP1) $\langle au + bv, w\rangle = a^*\langle u, w\rangle + b^*\langle v, w\rangle$;
(IP2) $\langle u, v\rangle = \langle v, u\rangle^*$;
(IP3) $\langle u, u\rangle \ge 0$ and $\langle u, u\rangle = 0$ if and only if $u = 0$.

Using these properties, we also see that

$$\begin{aligned}\langle u, av + bw\rangle &= \langle av + bw, u\rangle^* \\ &= (a^*\langle v, u\rangle + b^*\langle w, u\rangle)^* \\ &= a\langle u, v\rangle + b\langle u, w\rangle\end{aligned}$$

and hence, for the sake of reference, we call this

(IP1′) $\langle u, av + bw\rangle = a\langle u, v\rangle + b\langle u, w\rangle$.

(The reader should be aware that instead of $\langle au, v\rangle = a^*\langle u, v\rangle$, many authors define $\langle au, v\rangle = a\langle u, v\rangle$ and $\langle u, av\rangle = a^*\langle u, v\rangle$. This is particularly true in mathematics texts, whereas we have chosen the convention used by most physics texts. Of course, this has no effect on any of our results.)

A space V together with an inner product is called an **inner product space**. If V is an inner product space over the field $\mathbb{C}$, then V is called a **complex** inner product space, and if the field is $\mathbb{R}$, then V is called a **real** inner product space. A complex inner product space is frequently called a **unitary space**, and a real inner product space is frequently called a **Euclidean space**. Note that in the case of a real space, the complex conjugates in (IP1) and (IP2) are superfluous.

By (IP2) we have $\langle u, u\rangle \in \mathbb{R}$ so that we may define the **length** (or **norm**) of u to be the nonnegative real number

$$\|u\| = \langle u, u\rangle^{1/2} .$$

If $\|u\| = 1$, then u is said to be a **unit vector**. If $\|v\| \neq 0$, then we can normalize v by setting $u = v/\|v\|$. One sometimes writes $\hat{v}$ to mean the unit vector in the direction of v, i.e., $v = \|v\|\,\hat{v}$.

Example 2.9 Let $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_n)$ be vectors in $\mathbb{C}^n$. We define

$$\langle X, Y\rangle = \sum_{i=1}^{n} x_i{}^* y_i$$

and leave it to the reader to show that this satisfies (IP1) – (IP3). In the case of the space $\mathbb{R}^n$, we have $\langle X, Y\rangle = X\bullet Y = \sum x_i y_i$. This inner product is called the **standard inner product** in $\mathbb{C}^n$ (or $\mathbb{R}^n$).

We also see that if $X, Y \in \mathbb{R}^n$ then

$$\|X - Y\|^2 = \langle X - Y, X - Y\rangle = \sum_{i=1}^{n} (x_i - y_i)^2 .$$

Thus $\|X - Y\|$ is indeed just the distance between the points $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_n)$ that we would expect by applying the Pythagorean theorem to points in $\mathbb{R}^n$. In particular, $\|X\|$ is simply the length of the vector X. ∕∕

It is now easy to see why we defined the inner product as we did. For example, consider simply the space $\mathbb{C}^3$. Then with respect to the standard inner product on $\mathbb{C}^3$, the vector X = (1, *i*, 0) will have norm $\|X\|^2 = \langle X, X\rangle = 1 + 1 + 0 = 2$, while if we had used the expression corresponding to the standard inner product on $\mathbb{R}^3$, we would have found $\|X\|^2 = 1 - 1 + 0 = 0$ even though $X \neq 0$.

Example 2.10 Let V be the vector space of continuous complex-valued functions defined on the real interval [a, b]. We may define an inner product on V by

$$\langle f, g\rangle = \int_a^b f^*(x)g(x)dx$$

for all f, g ∈ V. It should be obvious that this satisfies the three required properties of an inner product. //

We now prove the generalization of Theorem 0.7, an important result known as the **Cauchy-Schwartz inequality**.

Theorem 2.16 Let V be an inner product space. Then for any u, v ∈ V we have

$$|\langle u, v\rangle| \le \|u\|\,\|v\| \;.$$

Proof If either u or v is zero the theorem is trivially true. We therefore assume that $u \neq 0$ and $v \neq 0$. Then, for any real number c, we have (using (IP2) and the fact that $|z|^2 = zz^*$)

$$\begin{aligned}0 &\le \|v - c\langle u, v\rangle u\|^2\\ &= \langle v - c\langle u, v\rangle u,\; v - c\langle u, v\rangle u\rangle\\ &= \langle v, v\rangle - c\langle u, v\rangle\langle v, u\rangle - c\langle u, v\rangle^*\langle u, v\rangle + c^2\langle u, v\rangle^*\langle u, v\rangle\langle u, u\rangle\\ &= \|v\|^2 - 2c|\langle u, v\rangle|^2 + c^2|\langle u, v\rangle|^2\|u\|^2 .\end{aligned}$$

Now let $c = 1/\|u\|^2$ to obtain

$$0 \le \|v\|^2 - |\langle u, v\rangle|^2/\|u\|^2$$

or

$$|\langle u, v\rangle|^2 \le \|u\|^2\,\|v\|^2 \;.$$

Taking the square root proves the theorem. ∎

Theorem 2.17 The norm in an inner product space V has the following properties for all u, v ∈ V and k ∈ $\mathcal{F}$:

(N1) $\|u\| \geq 0$ and $\|u\| = 0$ if and only if u = 0.
(N2) $\|ku\| = |k|\,\|u\|$.
(N3) $\|u + v\| \leq \|u\| + \|v\|$.

Proof Since $\|u\| = \langle u, u\rangle^{1/2}$, (N1) follows from (IP3). Next, we see that

$$\|ku\|^2 = \langle ku, ku\rangle = |k|^2\,\|u\|^2$$

and hence taking the square root yields (N2). Finally, using Theorem 2.16 and the fact that z + z* = 2 Re z ≤ 2|z| for any z ∈ ℂ, we have

$$\begin{aligned}\|u+v\|^2 &= \langle u+v,\, u+v\rangle\\ &= \langle u,\, u\rangle + \langle u,\, v\rangle + \langle v,\, u\rangle + \langle v,\, v\rangle\\ &= \|u\|^2 + \langle u,\, v\rangle + \langle u,\, v\rangle^* + \|v\|^2\\ &\leq \|u\|^2 + 2\left|\langle u,\, v\rangle\right| + \|v\|^2\\ &\leq \|u\|^2 + 2\|u\|\|v\| + \|v\|^2\\ &= \left(\|u\| + \|v\|\right)^2.\end{aligned}$$

Taking the square root yields (N3). ∎

We note that property (N3) is frequently called the **triangle inequality** because in two or three dimensions, it simply says that the sum of two sides of a triangle is greater than the third. Furthermore, we remark that properties (N1) – (N3) may be used to *define* a normed vector space. In other words, a **normed vector space** is defined to be a vector space V together with a mapping $\|\ \|: V \to \mathbb{R}$ that obeys properties (N1) – (N3). While a normed space V does not in general have an inner product defined on it, the existence of an inner product leads in a natural way (i.e., by Theorem 2.17) to the existence of a norm on V.

Example 2.11 Let us prove a simple but useful result dealing with the norm in any normed space V. From the properties of the norm, we see that for any u, v ∈ V we have

$$\|u\| = \|u - v + v\| \leq \|u - v\| + \|v\|$$

and

$$\|v\| = \|v - u + u\| \leq \|u - v\| + \|u\|.$$

Rearranging each of these yields

$$\|u\| - \|v\| \le \|u - v\|$$

and

$$\|v\| - \|u\| \le \|u - v\|.$$

This shows that

$$\big|\, \|u\| - \|v\| \,\big| \le \|u - v\|. \quad /\!\!/$$

Example 2.12 Consider the space V of Example 2.10 and the associated inner product ⟨f, g⟩. Applying Theorem 2.16 we have

$$\left|\int_a^b f^*(x)g(x)dx\right| \le \left\{\int_a^b |f(x)|^2\,dx\right\}^{1/2} \left\{\int_a^b |g(x)|^2\,dx\right\}^{1/2}$$

and applying Theorem 2.17 we see that

$$\left\{\int_a^b |f(x)+g(x)|^2\,dx\right\}^{1/2} \le \left\{\int_a^b |f(x)|^2\,dx\right\}^{1/2} + \left\{\int_a^b |g(x)|^2\,dx\right\}^{1/2}.$$

The reader might try and prove either of these directly from the definition of the integral if he or she wants to gain an appreciation of the power of the axiomatic approach to inner products. ∕∕

Finally, let us finish our generalization of Lemmas 2.1 - 2.3. If we repeat the proof of Lemma 2.3 using the inner product and norm notations, we find that for any u, v ∈ $\mathbb{R}^3$ we have ⟨u, v⟩ = ‖u‖ ‖v‖ cos θ. Now let V be any real vector space. We define the **angle** θ between two nonzero vectors u, v ∈ V by

$$\cos\theta = \frac{\langle u, v\rangle}{\|u\|\|v\|}.$$

Note that |cos θ| ≤ 1 by Theorem 2.16 so that this definition makes sense. We say that u is **orthogonal** (or **perpendicular**) to v if ⟨u, v⟩ = 0. If u and v are orthogonal, we often write this as u ⊥ v. From the basic properties of the inner product, it then follows that ⟨v, u⟩ = ⟨u, v⟩* = 0* = 0 so that v is orthogonal to u also. Thus u ⊥ v if and only if cos θ = 0. While cos θ is only defined in a real vector space, our definition of orthogonality is valid in any space V over $\mathcal{F}$.

Exercises

1. Let $x = (x_1, x_2)$ and $y = (y_1, y_2)$ be vectors in $\mathbb{R}^2$, and define the mapping $\langle\ ,\ \rangle: \mathbb{R}^2 \to \mathbb{R}$ by $\langle x, y\rangle = x_1y_1 - x_1y_2 - x_2y_1 + 3x_2y_2$. Show that this defines an inner product on $\mathbb{R}^2$.

2. Let $x = (3, 4) \in \mathbb{R}^2$, and evaluate $\|x\|$ with respect to the norm induced by:
(a) The standard inner product on $\mathbb{R}^2$.
(b) The inner product defined in the previous exercise.

3. Let V be an inner product space, and let $x, y \in V$.
(a) Prove the **parallelogram law**:

$$\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2 .$$

(The geometric meaning of this equation is that the sum of the squares of the diagonals of a parallelogram is equal to the sum of the squares of the sides.)
(b) Prove the **Pythagorean theorem**:

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 \quad \text{if } x \perp y .$$

4. Find a unit vector orthogonal to the vectors $x = (1, 1, 2)$ and $y = (0, 1, 3)$ in $\mathbb{R}^3$.

5. Let $u = (z_1, z_2)$ and $v = (w_1, w_2)$ be vectors in $\mathbb{C}^2$, and define the mapping $\langle\ ,\ \rangle: \mathbb{C}^2 \to \mathbb{R}$ by

$$\langle u, v\rangle = z_1w_1{}^* + (1 + i)z_1w_2{}^* + (1 - i)z_2w_1{}^* + 3z_2w_2{}^* .$$

Show that this defines an inner product on $\mathbb{C}^2$.

6. Let $u = (1 - 2i, 2 + 3i) \in \mathbb{C}^2$ and evaluate $\|u\|$ with respect to the norm induced by:
(a) The standard norm on $\mathbb{C}^2$.
(b) The inner product defined in the previous exercise.

7. Let V be an inner product space. Verify the following polar form identities:
(a) If V is a real space and $x, y \in V$, then

$$\langle x, y\rangle = (1/4)(\|x + y\|^2 - \|x - y\|^2) \ .$$

(b) If V is a complex space and x, y ∈ V, then

$$\langle x, y\rangle = (1/4)(\|x + y\|^2 - \|x - y\|^2) + (i/4)(\|i\, x + y\|^2 - \|ix - y\|^2)$$

(If we were using instead the inner product defined by $\langle \alpha x, y\rangle = \alpha\langle x, y\rangle$, then the last two terms in this equation would read $\|x \pm iy\|$.)

8. Let V = C[0, 1] be the space of continuous real-valued functions defined on the interval [0, 1]. Define an inner product on C[0, 1] by
$$\langle f, g\rangle = \int_0^1 f(t)g(t)dt.$$
(a) Verify that this does indeed define an inner product on V.
(b) Evaluate $\|f\|$ where $f = t^2 - 2t + 3 \in V$.

9. Given a vector space V, we define a mapping d: V × V → ℝ by $d(x, y) = \|x - y\|$ for all x, y ∈ V. Show that:
(a) $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$.
(b) $d(x, y) = d(y, x)$.
(c) $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality).
The number d(x, y) is called the **distance** from x to y, and the mapping d is called a **metric** on V. Any arbitrary set S on which we have defined a function d: S × S → ℝ satisfying these three properties is called a **metric space**.

10. Let $\{e_1, \dots, e_n\}$ be an orthonormal basis for a complex space V, and let x ∈ V be arbitrary. Show that
(a) $x = \sum_{i=1}^{n} e_i \langle e_i, x\rangle$.
(b) $\|x\|^2 = \sum_{i=1}^{n} |\langle e_i, x\rangle|^2$.

11. Show equality holds in the Cauchy-Schwartz inequality if and only if one vector is proportional to the other.

2.5 ORTHOGONAL SETS

If a vector space V is equipped with an inner product, then we may define a subspace of V that will turn out to be extremely useful in a wide variety of applications. Let W be any subset of such a vector space V. (Note that W need not be a subspace of V.) We define the **orthogonal compliment** of W to be the set $W^\perp$ given by

$$W^\perp = \{v \in V: \langle v, w \rangle = 0 \text{ for all } w \in W\} \;.$$

Theorem 2.18 Let W be any subset of a vector space V. Then $W^\perp$ is a subspace of V.

Proof We first note that $0 \in W^\perp$ since for any $v \in V$ we have

$$\langle 0, v \rangle = \langle 0v, v \rangle = 0\langle v, v \rangle = 0 \;.$$

To finish the proof, we simply note that for any $u, v \in W^\perp$, for any scalars a, $b \in \mathcal{F}$, and for every $w \in W$ we have

$$\langle au + bv, w \rangle = a^*\langle u, w \rangle + b^*\langle v, w \rangle = a^*0 + b^*0 = 0$$

so that $au + bv \in W^\perp$. ∎

Consider the space $\mathbb{R}^3$ with the usual Cartesian coordinate system (x, y, z). If we let $W = \mathbb{R}^2$ be the xy-plane, then $W^\perp = \mathbb{R}^1$ is just the z-axis since the standard inner product on $\mathbb{R}^3$ shows that any $v \in \mathbb{R}^3$ of the form (0, 0, c) is orthogonal to any $w \in \mathbb{R}^3$ of the form (a, b, 0). Thus, in this case anyway, we see that $W \oplus W^\perp = \mathbb{R}^3$. We will shortly prove that $W \oplus W^\perp = V$ for any inner product space V and subspace $W \subset V$. Before we can do this however, we must first discuss orthonormal sets of vectors.

A set $\{v_i\}$ of nonzero vectors in a space V is said to be an **orthogonal set** (or to be **mutually orthogonal**) if $\langle v_i, v_j \rangle = 0$ for $i \neq j$. If in addition, each v_i is a unit vector, then the set $\{v_i\}$ is said to be an **orthonormal set** and we write

$$\langle v_i, v_j \rangle = \delta_{ij}$$

where the very useful symbol δ_{ij} (called the **Kronecker delta**) is defined by

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} .$$

Theorem 2.19 Any orthonormal set of vectors $\{v_i\}$ is linearly independent.

Proof If $\sum a_i v_i = 0$ for some set of scalars $\{a_i\}$, then

$$0 = \langle v_j, 0\rangle = \langle v_j, \Sigma a_i v_i\rangle = \Sigma_i\, a_i\langle v_j, v_i\rangle = \Sigma_i\, a_i\delta_{ij} = a_j$$

so that $a_j = 0$ for each j, and hence $\{v_i\}$ is linearly independent. ∎

Note that in the proof of Theorem 2.19 it was not really necessary that each v_i be a unit vector. Any orthogonal set would work just as well.

Theorem 2.20 If $\{v_1, v_2, \dots, v_n\}$ is an orthonormal set in V and if $w \in V$ is arbitrary, then the vector

$$u = w - \Sigma_i\, \langle v_i, w\rangle v_i$$

is orthogonal to each of the v_i.

Proof We simply compute $\langle v_j, u\rangle$:

$$\begin{aligned}\langle v_j, u\rangle &= \langle v_j, w - \Sigma_i\langle v_i, w\rangle v_i\rangle\\ &= \langle v_j, w\rangle - \Sigma_i\langle v_i, w\rangle\langle v_j, v_i\rangle\\ &= \langle v_j, w\rangle - \Sigma_i\langle v_i, w\rangle\delta_{ij}\\ &= \langle v_j, w\rangle - \langle v_j, w\rangle = 0\ .\ \blacksquare\end{aligned}$$

The numbers $c_i = \langle v_i, w\rangle$ are frequently called the **Fourier coefficients** of w with respect to v_i. In fact, we leave it as an exercise for the reader to show that the expression $\|w - \Sigma_i\, a_i v_i\|$ achieves its minimum precisely when $a_i = c_i$ (see Exercise 2.5.4). Furthermore, we also leave it to the reader (see Exercise 2.5.5) to show that

$$\sum_{i=1}^{n} |c_i|^2 \le \|w\|^2$$

which is called **Bessel's inequality**.

As we remarked earlier, most mathematics texts write $\langle u, av\rangle = a^*\langle u, v\rangle$ rather than $\langle u, av\rangle = a\langle u, v\rangle$. In this case, Theorem 2.20 would be changed to read that the vector

$$u = w - \Sigma_i\, \langle w, v_i\rangle v_i$$

is orthogonal to each v_j.

Example 2.13 The simplest and best known example of an orthonormal set is the set $\{e_i\}$ of standard basis vectors in $\mathbb{R}^n$. Thus

$$\begin{aligned} e_1 &= (1, 0, 0, \dots, 0) \\ e_2 &= (0, 1, 0, \dots, 0) \\ &\vdots \\ e_n &= (0, 0, 0, \dots, 1) \end{aligned}$$

and clearly

$$\langle e_i, e_j \rangle = e_i \bullet e_j = \delta_{ij}$$

since for any X = $(x_1, \dots, x_n)$ and Y = $(y_1, \dots, y_n)$ in $\mathbb{R}^n$, we have

$$\langle X, Y \rangle = X \bullet Y = \sum_{i=1}^{n} x_i y_i \ .$$

(It would perhaps be better to write the unit vectors as $\hat{e}_i$ rather than e_i, but this will generally not cause any confusion.) ∕∕

Example 2.14 Let V be the space of continuous complex-valued functions defined on the real interval [−π, π]. As in Example 2.10, we define

$$\langle f, g \rangle = \int_{-\pi}^{\pi} f^*(x) g(x)\, dx$$

for all f, g ∈ V. We show that the set of functions

$$f_n = \left(\frac{1}{2\pi}\right)^{1/2} e^{inx}$$

for n = 1, 2, . . . forms an orthonormal set.

If m = n, then

$$\langle f_m, f_n \rangle = \langle f_n, f_n \rangle = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{-inx} e^{inx}\, dx = \frac{1}{2\pi}\int_{-\pi}^{\pi} dx = 1 \ .$$

If m ≠ n, then we have

$$\begin{aligned} \langle f_m, f_n \rangle &= \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{-imx} e^{inx}\, dx = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{i(n-m)x}\, dx \\ &= \frac{1}{2\pi}\frac{e^{i(n-m)x}}{i(n-m)}\bigg|_{-\pi}^{\pi} \\ &= \frac{\sin(n-m)\pi}{\pi(n-m)} = 0 \end{aligned}$$

since sin nπ = 0 for any integer n. (Note that we also used the fact that

$$\sin\theta = \frac{1}{2i}\left(e^{i\theta} - e^{-i\theta}\right)$$

which follows from the Euler formula mentioned in Chapter 0.) Therefore, $\langle f_m, f_n\rangle = \delta_{mn}$. That the set $\{f_n\}$ is orthonormal is of great use in the theory of Fourier series. ∕∕

We now wish to show that every finite-dimensional vector space with an inner product has an orthonormal basis. The proof is based on the famous Gram-Schmidt orthogonalization process, the precise statement of which we present as a corollary following the proof.

Theorem 2.21 Let V be a finite-dimensional inner product space. Then there exists an orthonormal set of vectors that forms a basis for V.

Proof Let dim V = n and let $\{u_1, \dots, u_n\}$ be a basis for V. We will construct a new basis $\{w_1, \dots, w_n\}$ such that $\langle w_i, w_j\rangle = \delta_{ij}$. To begin, we choose

$$w_1 = u_1 / \|u_1\|$$

so that

$$\begin{aligned}\|w_1\|^2 &= \langle w_1, w_1\rangle = \langle u_1/\|u_1\|, u_1/\|u_1\|\rangle = (1/\|u_1\|^2)\langle u_1, u_1\rangle \\ &= (1/\|u_1\|^2)\|u_1\|^2 = 1\end{aligned}$$

and hence w_1 is a unit vector. We now take u_2 and subtract off its “projection” along w_1. This will leave us with a new vector v_2 that is orthogonal to w_1. Thus, we define

$$v_2 = u_2 - \langle w_1, u_2\rangle w_1$$

so that

$$\langle w_1, v_2\rangle = \langle w_1, u_2\rangle - \langle w_1, u_2\rangle\langle w_1, w_1\rangle = 0$$

(this also follows from Theorem 2.20). If we let

$$w_2 = v_2/\|v_2\|$$

then $\{w_1, w_2\}$ is an orthonormal set (that $v_2 \neq 0$ will be shown below).

We now go to u_3 and subtract off its projection along w_1 and w_2. In other words, we define

$$v_3 = u_3 - \langle w_2, u_3\rangle w_2 - \langle w_1, u_3\rangle w_1$$

so that $\langle w_1, v_3\rangle = \langle w_2, v_3\rangle = 0$. Choosing

$$w_3 = v_3/\|v_3\|$$

we now have an orthonormal set $\{w_1, w_2, w_3\}$.

It is now clear that given an orthonormal set $\{w_1, \ldots, w_k\}$, we let

$$v_{k+1} = u_{k+1} - \sum_{i=1}^{k} \langle w_i, u_{k+1}\rangle w_i$$

so that v_{k+1} is orthogonal to $w_1, \ldots, w_k$ (Theorem 2.20), and hence we define

$$w_{k+1} = v_{k+1}/\|v_{k+1}\| \; .$$

It should now be obvious that we can construct an orthonormal set of n vectors from our original basis of n vectors. To finish the proof, we need only show that $w_1, \ldots, w_n$ are linearly independent.

To see this, note first that since u_1 and u_2 are linearly independent, w_1 and u_2 must also be linearly independent, and hence $v_2 \neq 0$ by definition of linear independence. Thus w_2 exists and $\{w_1, w_2\}$ is linearly independent by Theorem 2.19. Next, $\{w_1, w_2, u_3\}$ is linearly independent since w_1 and w_2 are in the linear span of u_1 and u_2. Hence $v_3 \neq 0$ so that w_3 exists, and Theorem 2.19 again shows that $\{w_1, w_2, w_3\}$ is linearly independent.

In general then, if $\{w_1, \ldots, w_k\}$ is linearly independent, it follows that $\{w_1, \ldots, w_k, u_{k+1}\}$ is also independent since $\{w_1, \ldots, w_k\}$ is in the linear span of $\{u_1, \ldots, u_k\}$. Hence $v_{k+1} \neq 0$ and w_{k+1} exists. Then $\{w_1, \ldots, w_{k+1}\}$ is linearly independent by Theorem 2.19. Thus $\{w_1, \ldots, w_n\}$ forms a basis for V, and $\langle w_i, w_j\rangle = \delta_{ij}$. ∎

Corollary (**Gram-Schmidt process**) Let $\{u_1, \ldots, u_n\}$ be a linearly independent set of vectors in an inner product space V. Then there exists a set of orthonormal vectors $w_1, \ldots, w_n \in V$ such that the linear span of $\{u_1, \ldots, u_k\}$ is equal to the linear span of $\{w_1, \ldots, w_k\}$ for each $k = 1, \ldots, n$.

Proof This corollary follows by a careful inspection of the proof of Theorem 2.21. ∎

We emphasize that the Gram-Schmidt algorithm (the "orthogonalization process" of Theorem 2.21) as such applies to any inner product space, and is not restricted to only finite-dimensional spaces (see Chapter 12).

We are now ready to prove our earlier assertion. Note that here we require W to be a subspace of V.

Theorem 2.22 Let W be a subspace of a finite-dimensional inner product space V. Then $V = W \oplus W^\perp$.

Proof By Theorem 2.9, W is finite-dimensional. Therefore, if we choose a basis $\{v_1, \dots, v_k\}$ for W, it may be extended to a basis $\{v_1, \dots, v_n\}$ for V (Theorem 2.10). Applying Theorem 2.21 to this basis, we construct a new orthonormal basis $\{u_1, \dots, u_n\}$ for V where

$$u_r = \sum_{j=1}^{r} a_{rj} v_j$$

for $r = 1, \dots, n$ and some coefficients a_{rj} (determined by the Gram-Schmidt process). In particular, we see that $u_1, \dots, u_k$ are all in W, and hence they form an orthonormal basis for W.

Since $\{u_1, \dots, u_n\}$ are orthonormal, it follows that $u_{k+1}, \dots, u_n$ are in $W^\perp$ (since $\langle u_i, u_j \rangle = 0$ for all $i \le k$ and any $j = k + 1, \dots, n$). Therefore, given any $x \in V$ we have

$$x = a_1 u_1 + \cdots + a_n u_n$$

where

$$a_1 u_1 + \cdots + a_k u_k \in W$$

and

$$a_{k+1} u_{k+1} + \cdots + a_n u_n \in W^\perp .$$

This means that $V = W + W^\perp$, and we must still show that $W \cap W^\perp = \{0\}$. But if $y \in W \cap W^\perp$, then $\langle y, y \rangle = 0$ since $y \in W^\perp$ implies that y is orthogonal to any vector in W, and in particular, $y \in W$. Hence $y = 0$ by (IP3), and it therefore follows that $W \cap W^\perp = \{0\}$. ∎

Corollary If V is finite-dimensional and W is a subspace of V, then $(W^\perp)^\perp = W$.

Proof Given any $w \in W$ we have $\langle w, v \rangle = 0$ for all $v \in W^\perp$. This implies that $w \in (W^\perp)^\perp$ and hence $W \subset (W^\perp)^\perp$. By Theorem 2.22, $V = W \oplus W^\perp$ and hence

$$\dim V = \dim W + \dim W^\perp$$

(Theorem 2.11). But $W^\perp$ is also a subspace of V, and hence $V = W^\perp \oplus (W^\perp)^\perp$ (Theorem 2.22) which implies

$$\dim V = \dim W^\perp + \dim(W^\perp)^\perp .$$

Therefore, comparing these last two equations shows that $\dim W = \dim(W^\perp)^\perp$. This result together with $W \subset (W^\perp)^\perp$ implies that $W = (W^\perp)^\perp$. ∎

Finally, note that if $\{e_i\}$ is an orthonormal basis for V, then any $x \in V$ may be written as $x = \sum_i x_ie_i$ where

$$\langle e_j, x\rangle = \langle e_j, \textstyle\sum_i x_ie_i\rangle = \sum_i x_i\langle e_j, e_i\rangle = \sum_i x_i\delta_{ij} = x_j \;.$$

Therefore we may write

$$x = \textstyle\sum_i \langle e_i, x\rangle e_i$$

which is a very useful expression.

Example 2.15 Consider the following basis vectors for $\mathbb{R}^3$:

$$u_1 = (3, 0, 4) \quad u_2 = (-1, 0, 7) \quad u_3 = (2, 9, 11) \;.$$

Let us apply the Gram-Schmidt process (with the standard inner product on $\mathbb{R}^3$) to obtain a new orthonormal basis for $\mathbb{R}^3$. Since $\|u_1\| = \sqrt{9+16} = 5$, we define

$$w_1 = u_1/5 = (3/5, 0, 4/5) \;.$$

Next, using $\langle w_1, u_2\rangle = -3/5 + 28/5 = 5$ we let

$$v_2 = (-1, 0, 7) - (3, 0, 4) = (-4, 0, 3) \;.$$

Since $\|v_2\| = 5$, we have

$$w_2 = (-4/5, 0, 3/5) \;.$$

Finally, using $\langle w_1, u_3\rangle = 10$ and $\langle w_2, u_3\rangle = 5$ we let

$$v_3 = (2, 9, 11) - (-4, 0, 3) - (6, 0, 8) = (0, 9, 0)$$

and hence, since $\|v_3\| = 9$, our third basis vector becomes

$$w_3 = (0, 1, 0) \;.$$

We leave it to the reader to show that $\{w_1, w_2, w_3\}$ does indeed form an orthonormal basis for $\mathbb{R}^3$. ∫

We will have much more to say about inner product spaces after we have treated linear transformations in detail. For the rest of this book, unless explicitly stated otherwise, all vector spaces will be assumed to be finite-dimensional. In addition, the specific scalar field $\mathcal{F}$ will generally not be mentioned, but it is to be understood that all scalars are elements of $\mathcal{F}$.

Exercises

1. Let W be a subset of a vector space V. Prove the following:
   (a) $0^\perp = V$ and $V^\perp = 0$.
   (b) $W \cap W^\perp = \{0\}$.
   (c) $W_1 \subset W_2$ implies $W_2^\perp \subset W_1^\perp$.

2. Let U and W be subspaces of a finite-dimensional inner product space V. Prove the following:
   (a) $(U + W)^\perp = U^\perp \cap W^\perp$.
   (b) $(U \cap W)^\perp = U^\perp + W^\perp$.

3. Let $\{e_1, \dots, e_n\}$ be an orthonormal basis for an arbitrary inner product space V. If $u = \sum_i u_ie_i$ and $v = \sum_i v_ie_i$ are any vectors in V, show that

$$\langle u, v\rangle = \sum_{i=1}^n u_i * v_i$$

(this is just the generalization of Example 2.9).

4. Suppose $\{e_1, \dots, e_n\}$ is an orthonormal set in a vector space V, and x is any element of V. Show that the expression

$$\left\| x - \sum_{k=1}^n a_k e_k \right\|$$

achieves its minimum value when each of the scalars a_k is equal to the Fourier coefficient $c_k = \langle e_k, x\rangle$. [*Hint*: Using Theorem 2.20 and the Pythagorean theorem (see Exercise 2.4.3), add and subtract the term $\sum_{k=1}^n c_ke_k$ in the above expression to conclude that

$$\left\| x - \sum_{k=1}^n c_k e_k \right\|^2 \le \left\| x - \sum_{k=1}^n a_k e_k \right\|^2$$

for any set of scalars a_k.]

5. Let $\{e_1, \dots, e_n\}$ be an orthonormal set in an inner product space V, and let $c_k = \langle e_k, x\rangle$ be the Fourier coefficient of $x \in V$ with respect to e_k. Prove **Bessel's inequality**:

$$\sum_{k=1}^n |c_k|^2 \le \|x\|^2 \ .$$

[*Hint*: Use the definition of the norm along with the obvious fact that $0 \le \|x - \sum_{k=1}^{n} c_k e_k\|^2$.]

6. Find an orthonormal basis (relative to the standard inner product) for the following subspaces:

   (a) The subspace W of $\mathbb{C}^3$ spanned by the vectors $u_1 = (1, i, 0)$ and $u_2 = (1, 2, 1 - i)$.

   (b) The subspace W of $\mathbb{R}^4$ spanned by $u_1 = (1, 1, 0, 0)$, $u_2 = (0, 1, 1, 0)$ and $u_3 = (0, 0, 1, 1)$.

7. Consider the space $\mathbb{R}^3$ with the standard inner product.

   (a) Convert the vectors $u_1 = (1, 0, 1)$, $u_2 = (1, 0, -1)$ and $u_3 = (0, 3, 4)$ to an orthonormal basis $\{e_1, e_2, e_3\}$ of $\mathbb{R}^3$.

   (b) Write the components of an arbitrary vector $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ in terms of the basis $\{e_i\}$.

8. Let V = C[0, 1] be the inner product space defined in Exercise 2.4.8. Find an orthonormal basis for V generated by the functions $\{1, x, x^2, x^3\}$.

9. Let V and W be isomorphic inner product spaces under the vector space homomorphism ϕ: V → W, and assume that ϕ has the additional property that

$$\|\phi(x_1) - \phi(x_2)\| = \|x_1 - x_2\| \ .$$

   Such a ϕ is called an **isometry**, and V and W are said to be **isometric** spaces. (We also note that the norm on the left side of this equation is in W, while the norm on the right side is in V. We shall rarely distinguish between norms in different spaces unless there is some possible ambiguity.) Let V have orthonormal basis $\{v_1, \dots, v_n\}$ so that any $x \in V$ may be written as $x = \sum x_i v_i$. Prove that the mapping ϕ: V → $\mathbb{R}^n$ defined by $\phi(x) = (x_1, \dots, x_n)$ is an isometry of V onto $\mathbb{R}^n$ (with the standard inner product).

10. Let $\{e_1, e_2, e_3\}$ be an orthonormal basis for $\mathbb{R}^3$, and let $\{u_1, u_2, u_3\}$ be three mutually orthonormal vectors in $\mathbb{R}^3$. Let $u_\lambda{}^i$ denote the *ith* component of u_λ with respect to the basis $\{e_i\}$. Prove the **completeness relation**

$$\sum_{\lambda=1}^{3} u_\lambda{}^i u_\lambda{}^j = \delta_{ij} \ .$$

11. Let W be a finite-dimensional subspace of a possibly infinite-dimensional inner product space V. Prove that V = W ⊕ $W^\perp$. [*Hint*: Let $\{w_1, \dots, w_k\}$ be an orthonormal basis for W, and for any x ∈ V define

$$x_1 = \sum_{i=1}^{k} \langle w_i, x \rangle w_i$$

and $x_2 = x - x_1$. Show that $x_1 + x_2 \in W + W^\perp$, and that $W \cap W^\perp = \{0\}$.]

CHAPTER 3

Linear Equations and Matrices

In this chapter we introduce matrices via the theory of simultaneous linear equations. This method has the advantage of leading in a natural way to the concept of the reduced row-echelon form of a matrix. In addition, we will formulate some of the basic results dealing with the existence and uniqueness of systems of linear equations. In Chapter 5 we will arrive at the same matrix algebra from the viewpoint of linear transformations.

3.1 SYSTEMS OF LINEAR EQUATIONS

Let $a_1, \dots, a_n, y$ be elements of a field $\mathcal{F}$, and let $x_1, \dots, x_n$ be **unknowns** (also called **variables** or **indeterminates**). Then an equation of the form

$$a_1 x_1 + \cdots + a_n x_n = y$$

is called a **linear equation in n unknowns** (over $\mathcal{F}$). The scalars a_i are called the **coefficients** of the unknowns, and y is called the **constant term** of the equation. A vector $(c_1, \dots, c_n) \in \mathcal{F}^n$ is called a **solution vector** of this equation if and only if

$$a_1 c_1 + \cdots + a_n c_n = y$$

in which case we say that $(c_1, \ldots, c_n)$ **satisfies** the equation. The set of all such solutions is called the **solution set** (or the **general solution**).

Now consider the following **system of m linear equations in n unknowns**:

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= y_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n &= y_2 \\ \vdots \qquad\quad \vdots \;\; &\;\; \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= y_m \end{aligned}$$

We abbreviate this system by

$$\sum_{j=1}^{n} a_{ij}x_j = y_i, \qquad i = 1, \ldots, m \ .$$

If we let S_i denote the solution set of the equation $\sum_j a_{ij}x_j = y_i$ for each i, then the solution set S of the system is given by the intersection $S = \cap S_i$. In other words, if $(c_1, \ldots, c_n) \in \mathcal{F}^n$ is a solution of the system of equations, then it is a solution of each of the m equations in the system.

Example 3.1 Consider this system of two equations in three unknowns over the real field $\mathbb{R}$:

$$\begin{aligned} 2x_1 - 3x_2 + x_3 &= 6 \\ x_1 + 5x_2 - 2x_3 &= 12 \end{aligned}$$

The vector $(3, 1, 3) \in \mathbb{R}^3$ is not a solution of this system because

$$2(3) - 3(1) + 3 = 6$$

while

$$3 + 5(1) - 2(3) = 2 \neq 12 \ .$$

However, the vector $(5, 1, -1) \in \mathbb{R}^3$ is a solution since

$$2(5) - 3(1) + (-1) = 6$$

and

$$5 + 5(1) - 2(-1) = 12 \ . \ /\!\!/$$

Associated with a system of linear equations are two rectangular arrays of elements of $\mathcal{F}$ that turn out to be of great theoretical as well as practical significance. For the system $\sum_j a_{ij}x_j = y_i$, we define the **matrix of coefficients** A as the array

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

and the **augmented matrix** as the array aug A given by

$$aug\ A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & y_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & y_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & y_n \end{pmatrix}\,.$$

In general, we will use the term **matrix** to denote any array such as the array A shown above. This matrix has m **rows** and n **columns**, and hence is referred to as an m x n matrix, or a matrix of **size** m x n. By convention, an element $a_{ij} \in \mathcal{F}$ of A is labeled with the first index referring to the row and the second index referring to the column. The scalar a_{ij} is usually called the i, *jth* **entry** (or **element**) of the matrix A. We will frequently denote the matrix A by the symbol (a_{ij}).

Another rather general way to define a matrix is as a mapping from a subset of all ordered pairs of positive integers into the field $\mathcal{F}$. In other words, we define the mapping A by $A(i, j) = a_{ij}$ for every $1 \le i \le m$ and $1 \le j \le n$. In this sense, a matrix is actually a mapping, and the m x n array written above is just a representation of this mapping.

Before proceeding with the general theory, let us give a specific example demonstrating how to solve a system of linear equations.

Example 3.2 Let us attempt to solve the following system of linear equations:

$$\begin{aligned} 2x_1 + x_2 - 2x_3 &= -3 \\ x_1 - 3x_2 + x_3 &= 8 \\ 4x_1 - x_2 - 2x_3 &= 3 \end{aligned}$$

That our approach is valid in general will be proved in our first theorem below.

Multiply the first equation by 1/2 to get the coefficient of x_1 equal to 1:

$$\begin{aligned} x_1 + (1/2)x_2 - x_3 &= -3/2 \\ x_1 - 3x_2 + x_3 &= 8 \\ 4x_1 - x_2 - 2x_3 &= 3 \end{aligned}$$

Multiply the first equation by −1 and add it to the second to obtain a new second equation, then multiply the first by −4 and add it to the third to obtain a new third equation:

$$\begin{aligned} x_1 + (1/2)x_2 - x_3 &= -3/2 \\ -(7/2)x_2 + 2x_3 &= 19/2 \\ -3x_2 - 2x_3 &= 9 \end{aligned}$$

Multiply the second by −2/7 to get the coefficient of x_2 equal to 1, then multiply this new second equation by 3 and add to the third:

$$\begin{aligned} x_1 + (1/2)x_2 - x_3 &= -3/2 \\ x_2 - (4/7)x_3 &= -19/7 \\ (2/7)x_3 &= 6/7 \end{aligned}$$

Multiply the third by 7/2, then add 4/7 times this new equation to the second:

$$\begin{aligned} x_1 + (1/2)x_2 - x_3 &= -3/2 \\ x_2 &= -1 \\ x_3 &= 3 \end{aligned}$$

Add the third equation to the first, then add −1/2 times the second equation to the new first to obtain

$$\begin{aligned} x_1 &= 2 \\ x_2 &= -1 \\ x_3 &= 3 \end{aligned}$$

This is now a solution of our system of equations. While this system could have been solved in a more direct manner, we wanted to illustrate the systematic approach that will be needed below. ∞

Two systems of linear equations are said to be **equivalent** if they have equal solution sets. That each successive system of equations in Example 3.2 is indeed equivalent to the previous system is guaranteed by the following theorem.

Theorem 3.1 The system of two equations in n unknowns over a field $\mathcal{F}$

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \end{aligned} \tag{1}$$

with $a_{11} \neq 0$ is equivalent to the system

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a'_{22}x_2 + \cdots + a'_{2n}x_n &= b'_2 \end{aligned} \tag{2}$$

in which

$$a'_{2i} = a_{21}\,a_{1i} - a_{11}\,a_{2i}$$

for each i = 1, . . . , n and

$$b'_2 = a_{21}\,b_1 - a_{11}\,b_2 \ .$$

Proof Let us define

$$L_i = \sum_{j=1}^{n} a_{ij}x_j$$

so that (1) may be written as the system

$$\begin{aligned} L_1 &= b_1 \\ L_2 &= b_2 \end{aligned} \tag{1$'$}$$

while (2) is just

$$\begin{aligned} L_1 &= b_1 \\ a_{21}L_1 - a_{11}L_2 &= a_{21}b_1 - a_{11}b_2 \end{aligned} \tag{2$'$}$$

If $(x_1, \ldots, x_n) \in \mathcal{F}^n$ is a solution of (1′), then the two equations

$$\begin{aligned} a_{21}L_1 &= a_{21}b_1 \\ a_{11}L_2 &= a_{11}b_2 \end{aligned}$$

and hence also

$$a_{21}\,L_1 - a_{11}\,L_2 = a_{21}\,b_1 - a_{11}\,b_2$$

are all true equations. Therefore every solution of (1′) also satisfies (2′).

Conversely, suppose that we have a solution $(x_1, \ldots, x_n)$ to the system (2′). Then clearly

$$a_{21}\,L_1 = a_{21}\,b_1$$

is a true equation. Hence, subtracting the second of (2′) from this gives us

$$a_{21}L_1 - (a_{21}L_1 - a_{11}L_2) = a_{21}b_1 - (a_{21}b_1 - a_{11}b_2)$$

or

$$a_{11}L_2 = a_{11}b_2 \ .$$

Thus $L_2 = b_2$ is also a true equation. This shows that any solution of (2′) is a solution of (1′) also. ∎

We point out that in the proof of Theorem 3.1 (as well as in Example 3.2), it was only the coefficients themselves that were of any direct use to us. The unknowns x_i were never actually used in any of the manipulations. This is the reason that we defined the matrix of coefficients (a_{ij}). What we now proceed to do is to generalize the above method of solving systems of equations in a manner that utilizes this matrix explicitly.

Exercises

1. For each of the following systems of equations, find a solution if it exists:

$$(a)\quad \begin{aligned} x+2y-3z&=-1\\ 3x-y+2z&=7\\ 5x+3y-4z&=2 \end{aligned} \qquad\qquad (b)\quad \begin{aligned} 2x+y-2z&=10\\ 3x+2y+2z&=1\\ 5x+4y+3z&=4 \end{aligned}$$

$$(c)\quad \begin{aligned} x+2y-3z&=6\\ 2x-y+4z&=2\\ 4x+3y-2z&=14 \end{aligned}$$

2. Determine whether or not the each of the following two systems is equivalent (over the complex field):

$$(a)\quad \begin{aligned} x-y&=0\\ 2x+y&=0 \end{aligned} \qquad \text{and} \qquad \begin{aligned} 3x+y&=0\\ x+y&=0 \end{aligned}$$

$$(b)\quad \begin{aligned} -x+y+4z&=0\\ x+3y+8z&=0\\ (1/2)x+y+(5/2)z&=0 \end{aligned} \qquad \text{and} \qquad \begin{aligned} x-z&=0\\ y+3z&=0 \end{aligned}$$

$$(c)\quad \begin{aligned} 2x+(-1+i)y+t&=0\\ 3y-2iz+5t&=0 \end{aligned}$$

and

$$\begin{aligned}(1+i/2)x+\quad 8y-iz-\ t&=0\\ (2/3)x-(1/2)y+z+7t&=0\end{aligned}$$

3.2 ELEMENTARY ROW OPERATIONS

The important point to realize in Example 3.2 is that we solved a system of linear equations by performing some combination of the following operations:

(a) Change the order in which the equations are written.
(b) Multiply each term in an equation by a nonzero scalar.
(c) Multiply one equation by a nonzero scalar and then add this new equation to another equation in the system.

Note that (a) was not used in Example 3.2, but it would have been necessary if the coefficient of x_1 in the first equation had been 0. The reason for this is that we want the equations put into echelon form as defined below.

We now see how to use the matrix aug A as a tool in solving a system of linear equations. In particular, we define the following so-called **elementary row operations** (or **transformations**) as applied to the augmented matrix:

(α) Interchange two rows.
(β) Multiply one row by a nonzero scalar.
(γ) Add a scalar multiple of one row to another.

It should be clear that operations (α) and (β) have no effect on the solution set of the system and, in view of Theorem 3.1, that operation (γ) also has no effect.

The next two examples show what happens both in the case where there is no solution to a system of linear equations, and in the case of an infinite number of solutions. In performing these operations on a matrix, we will let R_i denote the i*th* row. We leave it to the reader to repeat Example 3.2 using this notation.

Example 3.3 Consider this system of linear equations over the field $\mathbb{R}$:

$$\begin{aligned}x+3y+2z&=7\\ 2x+\ y-\ z&=5\\ -x+2y+3z&=4\end{aligned}$$

The augmented matrix is

$$\begin{pmatrix} 1 & 3 & 2 & 7 \\ 2 & 1 & -1 & 5 \\ -1 & 2 & 3 & 4 \end{pmatrix}$$

and the reduction proceeds as follows. We first perform the following elementary row operations:

$$\begin{array}{r} \\ R_2 - 2R_1 \rightarrow \\ R_3 + R_1 \rightarrow \end{array} \begin{pmatrix} 1 & 3 & 2 & 7 \\ 0 & -5 & -5 & -9 \\ 0 & 5 & 5 & 11 \end{pmatrix}$$

Now, using this matrix, we obtain

$$\begin{array}{r} \\ -R_2 \rightarrow \\ R_3 + R_2 \rightarrow \end{array} \begin{pmatrix} 1 & 3 & 2 & 7 \\ 0 & 5 & 5 & 9 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

It is clear that the equation 0z = 2 has no solution, and hence this system has no solution. ∕∕

Example 3.4 Let us solve the following system over the field ℝ:

$$\begin{aligned} x_1 - 2x_2 + 2x_3 - x_4 &= -14 \\ 3x_1 + 2x_2 - x_3 + 2x_4 &= 17 \\ 2x_1 + 3x_2 - x_3 - x_4 &= 18 \\ -2x_1 + 5x_2 - 3x_3 - 3x_4 &= 26 \end{aligned}$$

We have the matrix aug A given by

$$\begin{pmatrix} 1 & -2 & 2 & -1 & -14 \\ 3 & 2 & -1 & 2 & 17 \\ 2 & 3 & -1 & -1 & 18 \\ -2 & 5 & -3 & -3 & 26 \end{pmatrix}$$

and hence we obtain the sequence

$$\begin{array}{r} \\ R_2 - 3R_1 \rightarrow \\ R_3 - 2R_1 \rightarrow \\ R_4 + 2R_1 \rightarrow \end{array} \begin{pmatrix} 1 & -2 & 2 & -1 & -14 \\ 0 & 8 & -7 & 5 & 59 \\ 0 & 7 & -5 & 1 & 46 \\ 0 & 1 & 1 & -5 & -2 \end{pmatrix}$$

$$\begin{array}{r} \\ R_4 \to \\ R_2 - 8R_4 \to \\ R_3 - 7R_4 \to \end{array}\begin{pmatrix} 1 & -2 & 2 & -1 & -14 \\ 0 & 1 & 1 & -5 & -2 \\ 0 & 0 & -15 & 45 & 75 \\ 0 & 0 & -12 & 36 & 60 \end{pmatrix}$$

$$\begin{array}{r} \\ \\ (-1/15)R_3 \to \\ (-1/12)R_4 \to \end{array}\begin{pmatrix} 1 & -2 & 2 & -1 & -14 \\ 0 & 1 & 1 & -5 & -2 \\ 0 & 0 & 1 & -3 & -5 \\ 0 & 0 & 1 & -3 & -5 \end{pmatrix}$$

We see that the third and fourth equations are identical, and hence we have three equations in four unknowns:

$$\begin{aligned} x_1 - 2x_2 + 2x_3 - x_4 &= -14 \\ x_2 + x_3 - 5x_4 &= {-2} \\ x_3 - 3x_4 &= {-5} \end{aligned}$$

It is now apparent that there are an infinite number of solutions because, if we let $c \in \mathbb{R}$ be any real number, then our solution set is given by $x_4 = c$, $x_3 = 3c - 5$, $x_2 = 2c + 3$ and $x_1 = -c + 2$. //

Two m x n matrices are said to be **row equivalent** if one can be transformed into the other by a finite number of elementary row operations. We leave it to the reader to show that this defines an equivalence relation on the set of all m x n matrices (see Exercise 3.2.1).

Our next theorem is nothing more than a formalization of an earlier remark.

Theorem 3.2 Let A and B be the augmented matrices of two systems of m linear equations in n unknowns. If A is row equivalent to B, then both systems have the same solution set.

Proof If A is row equivalent to B, then we can go from the system represented by A to the system represented by B by a succession of the operations (a), (b) and (c) described above. It is clear that operations (a) and (b) have no effect on the solutions, and the method of Theorem 3.1 shows that operation (c) also has no effect. ∎

A matrix is said to be in **row-echelon form** if successive rows of the matrix start out (from the left) with more and more zeros. In particular, a matrix is said to be in **reduced row-echelon** form if it has the following properties (which are more difficult to state precisely than they are to understand):

(1) All zero rows (if any) occur below all nonzero rows.
(2) The first nonzero entry (reading from the left) in each row is equal to 1.
(3) If the first nonzero entry in the i*th* row is in the j_i*th* column, then every other entry in the j_i*th* column is 0.
(4) If the first nonzero entry in the i*th* row is in the j_i*th* column, then $j_1 < j_2 < \cdots$.

We will call the first (or **leading**) nonzero entries in each row of a row-echelon matrix the **distinguished elements** of the matrix. Thus, a matrix is in reduced row-echelon form if the distinguished elements are each equal to 1, and they are the only nonzero entries in their respective columns.

Example 3.5 The matrix

$$\begin{pmatrix} 1 & 2 & -3 & 0 & 1 \\ 0 & 0 & 5 & 2 & -4 \\ 0 & 0 & 0 & 7 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

is in row-echelon form but not in reduced row-echelon form. However, the matrix

$$\begin{pmatrix} 1 & 0 & 5 & 0 & 2 \\ 0 & 1 & 2 & 0 & 4 \\ 0 & 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

is in reduced row-echelon form. Note that the distinguished elements of the first matrix are the numbers 1, 5 and 7, and the distinguished elements of the second matrix are the numbers 1, 1 and 1. ∕∕

The algorithm detailed in the proof of our next theorem introduces a technique generally known as **Gaussian elimination**.

Theorem 3.3 Every m x n matrix A is row equivalent to a reduced row-echelon matrix.

Proof This is essentially obvious from Example 3.4. The detailed description which follows is an algorithm for determining the reduced row-echelon form of a matrix.

Suppose that we first put A into the form where the leading entry in each nonzero row is equal to 1, and where every other entry in the column containing this first nonzero entry is equal to 0. (This is called simply the **row-reduced** form of A.) If this can be done, then all that remains is to perform a finite number of row interchanges to achieve the final desired reduced row-echelon form.

To obtain the row-reduced form we proceed as follows. First consider row 1. If every entry in row 1 is equal to 0, then we do nothing with this row. If row 1 is nonzero, then let j_1 be the smallest positive integer for which $a_{1j_1} \neq 0$ and multiply row 1 by $(a_{1j_1})^{-1}$. Next, for each $i \neq 1$ we add $-a_{ij_1}$ times row 1 to row i. This leaves us with the leading entry a_{1j_1} of row 1 equal to 1, and every other entry in the j_1*th* column equal to 0.

Now consider row 2 of the matrix we are left with. Again, if row 2 is equal to 0 there is nothing to do. If row 2 is nonzero, assume that the first nonzero entry occurs in column j_2 (where $j_2 \neq j_1$ by the results of the previous paragraph). Multiply row 2 by $(a_{2j_2})^{-1}$ so that the leading entry in row 2 is equal to 1, and then add $-a_{ij_2}$ times row 2 to row i for each $i \neq 2$. Note that these operations have no effect on either column j_1, or on columns $1, \ldots, j_1$ of row 1.

It should now be clear that we can continue this process a finite number of times to achieve the final row-reduced form. We leave it to the reader to take an arbitrary matrix (a_{ij}) and apply successive elementary row transformations to achieve the desired final form. ∎

While we have shown that every matrix is row equivalent to at least one reduced row-echelon matrix, it is not obvious that this equivalence is unique. However, we shall show in the next section that this reduced row-echelon matrix is in fact unique. Because of this, the reduced row-echelon form of a matrix is often called the **row canonical form**.

Exercises

1. Show that row equivalence defines an equivalence relation on the set of all matrices.

2. For each of the following matrices, first reduce to row-echelon form, and then to row canonical form:

$$(a)\ \begin{pmatrix} 1 & -2 & 3 & -1 \\ 2 & -1 & 2 & 2 \\ 3 & 1 & 2 & 3 \end{pmatrix} \qquad (b)\ \begin{pmatrix} 1 & 2 & -1 & 2 & 1 \\ 2 & 4 & 1 & -2 & 3 \\ 3 & 6 & 2 & -6 & 5 \end{pmatrix}$$

$$(c)\ \begin{pmatrix} 1 & 3 & -1 & 2 \\ 0 & 1 & -5 & 3 \\ 2 & -5 & 3 & 1 \\ 4 & 1 & 1 & 5 \end{pmatrix}$$

3. For each of the following systems, find a solution or show that no solution exists:

$$(a)\ \begin{aligned} x+y+z&=1 \\ 2x-3y+7z&=0 \\ 3x-2y+8z&=4 \end{aligned} \qquad (b)\ \begin{aligned} x-y+2z&=1 \\ x+y+z&=2 \\ 2x-y+z&=5 \end{aligned}$$

$$(c)\ \begin{aligned} x-y+2z&=4 \\ 3x+y+4z&=6 \\ x+y+z&=1 \end{aligned} \qquad (d)\ \begin{aligned} x+3y+z&=2 \\ 2x+7y+4z&=6 \\ x+y-4z&=1 \end{aligned}$$

$$(e)\ \begin{aligned} x+3y+z&=0 \\ 2x+7y+4z&=0 \\ x+y-4z&=0 \end{aligned} \qquad (f)\ \begin{aligned} 2x-y+5z&=19 \\ x+5y-3z&=4 \\ 3x+2y+4z&=5 \end{aligned}$$

$$(g)\ \begin{aligned} 2x-y+5z&=19 \\ x+5y-3z&=4 \\ 3x+2y+4z&=25 \end{aligned}$$

4. Let f_1, f_2 and f_3 be elements of $F[\mathbb{R}]$ (i.e., the space of all real-valued functions defined on $\mathbb{R}$).

(a) Given a set $\{x_1, x_2, x_3\}$ of real numbers, define the 3 x 3 matrix $F(x) = (f_i(x_j))$ where the rows are labelled by i and the columns are labelled by j. Prove that the set $\{f_i\}$ is linearly independent if the rows of the matrix $F(x)$ are linearly independent.

(b) Now assume that each f_i has first and second derivatives defined on some interval $(a, b) \subset \mathbb{R}$, and let $f_i^{(j)}$ denote the *jth* derivative of f_i (where $f_i^{(0)}$ is just f_i). Define the matrix $W(x) = (f_i^{(j-1)}(x))$ where $1 \le i, j \le 3$. Prove that $\{f_i\}$ is linearly independent if the rows of $W(x)$ are independent for some x ∈ (a, b). (The determinant of W(x) is called the **Wronskian** of the set of functions $\{f_i\}$.)

Show that each of the following sets of functions is linearly independent:

(c) $f_1(x) = -x^2 + x + 1$, $f_2(x) = x^2 + 2x$, $f_3(x) = x^2 - 1$.

(d) $f_1(x) = \exp(-x)$, $f_2(x) = x$, $f_3(x) = \exp(2x)$.

(e) $f_1(x) = \exp(x)$, $f_2(x) = \sin x$, $f_3(x) = \cos x$.

5. Let

$$A = \begin{pmatrix} 3 & -1 & 2 \\ 2 & 1 & 1 \\ 1 & -3 & 0 \end{pmatrix} .$$

Determine the values of $Y = (y_1, y_2, y_3)$ for which the system $\sum_i a_{ij}x_j = y_i$ has a solution.

6. Repeat the previous problem with the matrix

$$A = \begin{pmatrix} 3 & -6 & 2 & -1 \\ -2 & 4 & 1 & 3 \\ 0 & 0 & 1 & 1 \\ 1 & -2 & 1 & 0 \end{pmatrix} .$$

3.3 ROW AND COLUMN SPACES

We will find it extremely useful to consider the rows and columns of an arbitrary m x n matrix as vectors in their own right. In particular, the rows of A are to be viewed as vector n-tuples $A_1, \dots, A_m$ where each $A_i = (a_{i1}, \dots, a_{in}) \in \mathcal{F}^n$. Similarly, the columns of A are to be viewed as vector m-tuples $A^1, \dots, A^n$ where each $A^j = (a_{1j}, \dots, a_{mj}) \in \mathcal{F}^m$. For notational clarity, we should write A^j as the column vector

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

but it is typographically easier to write this horizontally whenever possible. Note that we label the row vectors of A by subscripts, and the columns of A by superscripts.

Since each row A_i is an element of $\mathcal{F}^n$, the set of all rows of a matrix can be used to generate a new vector space V over $\mathcal{F}$. In other words, V is the space spanned by the rows A_i, and hence any $v \in V$ may be written as

$$v = \sum_{i=1}^{m} c_i A_i$$

where each $c_i \in \mathcal{F}$. The space V (which is apparently a subspace of $\mathcal{F}^n$) is called the **row space** of A. The dimension of V is called the **row rank** of A, and will be denoted by rr(A). Since V is a subspace of $\mathcal{F}^n$ and $\dim \mathcal{F}^n = n$, it follows that $\text{rr}(A) = \dim V \le n$. On the other hand, V is spanned by the m vectors A_i, so that we must have $\dim V \le m$. It then follows that $\text{rr}(A) \le \min\{m, n\}$.

In an exactly analogous manner, we define the column space W of a matrix A as that subspace of $\mathcal{F}^m$ spanned by the n column vectors A^j. Thus any $w \in W$ is given by

$$w = \sum_{j=1}^{n} b_j A^j$$

The **column rank** of A, denoted by cr(A), is given by $\text{cr}(A) = \dim W$ and, as above, we must have $\text{cr}(A) \le \min\{m, n\}$.

An obvious question is whether a sequence of elementary row operations changes either the row space or the column space of a matrix. A moments thought should convince you that the row space should not change, but it may not be clear exactly what happens to the column space. These questions are answered in our next theorem. While the following proof appears to be rather long, it is actually quite simple to understand.

Theorem 3.4 Let A and $\tilde{A}$ be row equivalent m x n matrices. Then the row space of A is equal to the row space of $\tilde{A}$, and hence $\text{rr}(A) = \text{rr}(\tilde{A})$. Furthermore, we also have $\text{cr}(A) = \text{cr}(\tilde{A})$. (However, note that the column space of A is not necessarily the same as the column space of $\tilde{A}$.)

Proof Let V be the row space of A and $\tilde{V}$ the row space of $\tilde{A}$. Since A and $\tilde{A}$ are row equivalent, A may be obtained from $\tilde{A}$ by applying successive elementary row operations. But then each row of A is a linear combination of rows of $\tilde{A}$, and hence $V \subset \tilde{V}$. On the other hand, $\tilde{A}$ may be obtained from A in a similar manner so that $\tilde{V} \subset V$. Therefore $V = \tilde{V}$ and hence $\text{rr}(A) = \text{rr}(\tilde{A})$.

Now let W be the column space of A and $\tilde{W}$ the column space of $\tilde{A}$. Under elementary row operations, it will not be true in general that $W = \tilde{W}$, but we will show it is still always true that $\dim W = \dim \tilde{W}$. Let us define the mapping $f: W \to \tilde{W}$ by

$$f\left(\sum_{i=1}^{n} c_i A^i\right) = \sum_{i=1}^{n} c_i \tilde{A}^i \ .$$

In other words, if we are given any linear combination of the columns of A, then we look at the same linear combination of columns of $\tilde{A}$. In order to show that this is well-defined, we must show that if $\Sigma a_i A^i = \Sigma b_i A^i$, then $f(\Sigma a_i A^i) = f(\Sigma b_i A^i)$. This equivalent to showing that if $\Sigma c_i A^i = 0$ then $f(\Sigma c_i A^i) = 0$ because if $\Sigma(a_i - b_i)A^i = 0$ and $f(\Sigma(a_i - b_i)A^i) = 0$, then

$$\begin{aligned} 0 &= f\big(\Sigma(a_i - b_i)A^i\big) = \Sigma(a_i - b_i)\tilde{A}^i = \Sigma a_i\tilde{A}^i - \Sigma b_i\tilde{A}^i \\ &= f\big(\Sigma a_i A^i\big) - f\big(\Sigma b_i A^i\big) \end{aligned}$$

and therefore

$$f(\Sigma a_i A^i) = f(\Sigma b_i A^i) \ .$$

Now note that

$$\begin{aligned} f\big(\Sigma(b_i A^i + c_i A^i)\big) &= f\big(\Sigma(b_i + c_i)A^i\big) = \Sigma(b_i + c_i)\tilde{A}^i \\ &= \Sigma b_i\tilde{A}^i + \Sigma c_i\tilde{A}^i = f\big(\Sigma b_i A^i\big) + f\big(\Sigma c_i A^i\big) \end{aligned}$$

and

$$f(k(\Sigma c_i A^i)) = f(\Sigma(kc_i)A^i) = \Sigma(kc_i)\,\tilde{A}^i = kf(\Sigma c_i A^i)$$

so that f is a vector space homomorphism. If we can show that W and $\tilde{W}$ are isomorphic, then we will have $cr(A) = \dim W = \dim \tilde{W} = cr(\tilde{A})$. Since f is clearly surjective, we need only show that Ker f = {0} for each of the three elementary row transformations.

In the calculations to follow, it must be remembered that

$$A_i = (a_{i1}, \dots, a_{in})$$

and

$$A^i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix} .$$

Since

$$\Sigma c_i A_i = (\Sigma c_i a_{i1}, \dots, \Sigma c_i a_{in})$$

we see that $\Sigma c_i A_i = 0$ if and only if $\Sigma c_i a_{ij} = 0$ for every $j = 1, \dots, n$. Similarly,

$$\Sigma c_i A^i = (\Sigma c_i a_{1i}, \dots, \Sigma c_i a_{mi})$$

so that $\Sigma c_i A^i = 0$ if and only if $\Sigma c_i a_{ji} = 0$ for every $j = 1, \dots, m$ (remember that we usually write a column vector in the form of a row vector).

We first consider a transformation of type α. For definiteness, we interchange rows 1 and 2, although it will be obvious that any pair of rows will work. In other words, we define $\tilde{A}_1 = A_2$, $\tilde{A}_2 = A_1$ and $\tilde{A}_j = A_j$ for $j = 3, \dots, n$. Therefore

$$f(\Sigma c_i A^i) = \Sigma c_i \tilde{A}^i = (\Sigma c_i a_{2i}, \Sigma c_i a_{1i}, \Sigma c_i a_{3i}, \dots, \Sigma c_i a_{mi}) \ .$$

If

$$\Sigma c_i A^i = 0$$

then

$$\Sigma c_i a_{ji} = 0$$

for every $j = 1, \dots, m$ and hence we see that $f(\Sigma c_i A^i) = 0$. This shows that f is well-defined for type α transformations. Conversely, if

$$f(\Sigma c_i A^i) = 0$$

then we see that again

$$\Sigma c_i a_{ji} = 0$$

for every $j = 1, \dots, m$ since each component in the expression $\Sigma c_i \tilde{A}^i = 0$ must equal 0. Hence $\Sigma c_i A^i = 0$ if and only if $f(\Sigma c_i A^i) = 0$, and hence Ker f = {0} for type α transformations (which also shows that f is well-defined).

We leave it to the reader (see Exercise 3.3.1) to show that f is well-defined and Ker f = {0} for transformations of type β, and we go on to those of type γ. Again for definiteness, we consider the particular transformation $\tilde{A}_1 = A_1 + kA_2$ and $\tilde{A}_j = A_j$ for $j = 2, \dots, m$. Then

$$\begin{aligned} f\left(\Sigma c_i A^i\right) &= \Sigma c_i \tilde{A}^i = \Sigma c_i \left(a_{1i} + k a_{2i}, a_{2i}, \dots, a_{mi}\right) \\ &= \left(\Sigma c_i a_{1i} + \Sigma k c_i a_{2i}, \Sigma c_i a_{2i}, \dots, \Sigma c_i a_{mi}\right) \end{aligned}$$

If

$$\Sigma c_i A^i = 0$$

then

$$\Sigma c_i a_{ji} = 0$$

for every $j = 1, \dots, m$ so that $\Sigma c_i \tilde{A}^i = 0$ and f is well-defined for type γ transformations. Conversely, if

$$\Sigma c_i \tilde{A}^i = 0$$

then

$$\Sigma c_i a_{ji} = 0$$

for j = 2, . . . , m, and this then shows that $\sum c_i a_{1i} = 0$ also. Thus $\sum c_i \tilde{A}^i = 0$ implies that $\sum c_i A^i = 0$, and hence $\sum c_i A^i = 0$ if and only if $f(\sum c_i A^i) = 0$. This shows that Ker f = {0} for type γ transformations also, and f is well-defined.

In summary, by constructing an explicit isomorphism in each case, we have shown that the column spaces W and $\tilde{W}$ are isomorphic under all three types of elementary row operations, and hence it follows that the column spaces of row equivalent matrices must have the same dimension. ∎

Corollary If $\tilde{A}$ is the row-echelon form of A, then $\sum c_i A^i = 0$ if and only if $\sum c_i \tilde{A}^i = 0$.

Proof This was shown explicitly in the proof of Theorem 3.4 for each type of elementary row operation. ∎

In Theorem 3.3 we showed that every matrix is row equivalent to a reduced row-echelon matrix, and hence (by Theorem 3.4) any matrix and its row canonical form have the same row space. Note though, that if the original matrix has more rows than the dimension of its row space, then the rows obviously can not all be linearly independent. However, we now show that the nonzero rows of the row canonical form are in fact linearly independent, and hence form a basis for the row space.

Theorem 3.5 The nonzero row vectors of an m x n reduced row-echelon matrix R form a basis for the row space of R.

Proof From the four properties of a reduced row-echelon matrix, we see that if R has r nonzero rows, then there exist integers $j_1, \dots, j_r$ with each $j_i \le n$ and $j_1 < \cdots < j_r$ such that R has a 1 in the *ith* row and j_i*th* column, and every other entry in the j_i*th* column is 0 (it may help to refer to Example 3.5 for visualization). If we denote these nonzero row vectors by $R_1, \dots, R_r$ then any arbitrary vector

$$v = \sum_{i=1}^{r} c_i R_i$$

has c_i as its j_i*th* coordinate (note that v may have more than r coordinates if r < n). Therefore, if v = 0 we must have each coordinate of v equal to 0, and hence $c_i = 0$ for each i = 1, . . . , r. But this means that the R_i are linearly independent, and since $\{R_i\}$ spans the row space by definition, we see that they must in fact form a basis. ∎

Corollary If A is any matrix and R is a reduced row-echelon matrix row equivalent to A, then the nonzero row vectors of R form a basis for the row space of A.

Proof In Theorem 3.4 we showed that A and R have the same row space. The corollary now follows from Theorem 3.5. ∎

Example 3.6 Let us determine whether or not the following matrices have the same row space:

$$A = \begin{pmatrix} 1 & 2 & -1 & 3 \\ 2 & 4 & 1 & -2 \\ 3 & 6 & 3 & -7 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 2 & -4 & 11 \\ 2 & 4 & -5 & 14 \end{pmatrix}\,.$$

We leave it to the reader to show (and you really should do it) that the reduced row-echelon form of these matrices is

$$A = \begin{pmatrix} 1 & 2 & 0 & 1/3 \\ 0 & 0 & 1 & -8/3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 2 & 0 & 1/3 \\ 0 & 0 & 1 & -8/3 \end{pmatrix}\,.$$

Since the the nonzero rows of the reduced row-echelon form of A and B are identical, the row spaces must be the same. ///

Now that we have a better understanding of the row space of a matrix, let us go back and show that the reduced row-echelon form of a given matrix is unique. We first prove a preliminary result dealing with the row-echelon form of two matrices having the same row space.

Theorem 3.6 Let $A = (a_{ij})$ be a row-echelon matrix with distinguished elements $a_{1j_1}, a_{2j_2}, \dots, a_{rj_r}$ and let $B = (b_{ij})$ be another row-echelon matrix with distinguished elements $b_{1k_1}, b_{2k_2}, \dots, b_{sk_s}$. Assume that A and B have the same row space (and therefore the same number of columns). Then the distinguished elements of A are in the same position as those of B, i.e., $r = s$ and $j_1 = k_1, j_2 = k_2, \dots, j_r = k_r$.

Proof Since $A = 0$ if and only if $B = 0$, we need only consider the nontrivial case where $r \geq 1$ and $s \geq 1$. First suppose that $j_1 < k_1$. This means that the j_1th column of B is equal to $(0, \dots, 0)$. Since A and B have the same row space, the first row of A is just a linear combination of the rows of B. In particular, we then have $a_{1j_1} = \sum_i c_i b_{ij_1}$ for some set of scalars c_i (see the proof of

Theorem 3.4). But $b_{ij_1} = 0$ for every i, and hence $a_{1j_1} = 0$ which contradicts the assumption that a_{1j_1} is a distinguished element of A (and must be nonzero by definition). We are thus forced to conclude that $j_1 \geq k_1$. However, we could clearly have started with the assumption that $k_1 < j_1$, in which case we would have been led to conclude that $k_1 \geq j_1$. This shows that we must actually have $j_1 = k_1$.

Now let A′ and B′ be the matrices which result from deleting the first row of A and B respectively. If we can show that A′ and B′ have the same row space, then they will also satisfy the hypotheses of the theorem, and our conclusion follows at once by induction.

Let $R = (a_1, a_2, \dots, a_n)$ be any row of A′ (and hence a row of A), and let $B_1, \dots, B_m$ be the rows of B. Since A and B have the same row space, we again have

$$R = \sum_{i=1}^{m} d_i B_i$$

for some set of scalars d_i. Since R is not the first row of A and A′ is in row-echelon form, it follows that $a_i = 0$ for $i = j_1 = k_1$. In addition, the fact that B is in row-echelon form means that every entry in the k_1*th* column of B must be 0 except for the first, i.e., $b_{1k_1} \neq 0$, $b_{2k_1} = \cdots = b_{mk_1} = 0$. But then

$$0 = a_{k_1} = d_1 b_{1k_1} + d_2 b_{2k_1} + \cdots + d_m b_{mk_1} = d_1 b_{1k_1}$$

which implies that $d_1 = 0$ since $b_{1k_1} \neq 0$. This shows that R is actually a linear combination of the rows of B′, and hence (since R was arbitrary) the row space of A′ must be a subspace of the row space of B′. This argument can clearly be repeated to show that the row space of B′ is a subspace of the row space of A′, and hence we have shown that A′ and B′ have the same row space. ∎

Theorem 3.7 Let $A = (a_{ij})$ and $B = (b_{ij})$ be reduced row-echelon matrices. Then A and B have the same row space if and only if they have the same nonzero rows.

Proof Since it is obvious that A and B have the same row space if they have the same nonzero rows, we need only prove the converse. So, suppose that A and B have the same row space. Then if A_i is an arbitrary nonzero row of A, we may write

$$A_i = \Sigma_r c_r B_r \qquad (1)$$

where the B_r are the nonzero rows of B. The proof will be finished if we can show that $c_r = 0$ for $r \neq i$ and $c_i = 1$.

To show that $c_i = 1$, let a_{ij_i} be the first nonzero entry in A_i, i.e., a_{ij_i} is the distinguished element of the *i*th row of A. Looking at the j_i*th* component of (1) we see that

$$a_{ij_i} = \Sigma_r c_r b_{rj_i} \tag{2}$$

(see the proof of Theorem 3.4). From Theorem 3.6 we know that b_{ij_i} is the distinguished element of the *i*th row of B, and hence it is the only nonzero entry in the j_i*th* column of B (by definition of a reduced row-echelon matrix). This means that (2) implies $a_{ij_i} = c_i\, b_{ij_i}$. In fact, it must be true that $a_{ij_i} = b_{ij_i} = 1$ since A and B are reduced row-echelon matrices, and therefore $c_i = 1$.

Now let b_{kj_k} be the first nonzero entry of B_k (where $k \neq i$). From (1) again we have

$$a_{ij_k} = \Sigma_r c_r b_{rj_k} \ . \tag{3}$$

Since B is a reduced row-echelon matrix, $b_{kj_k} = 1$ is the only nonzero entry in the j_k*th* column of B, and hence (3) shows us that $a_{ij_k} = c_k b_{kj_k}$. But from Theorem 3.6, a_{kj_k} is a distinguished element of A, and hence the fact that A is row-reduced means that $a_{ij_k} = 0$ for $i \neq k$. This forces us to conclude that $c_k = 0$ for $k \neq i$ as claimed. ∎

Suppose that two people are given the same matrix A and asked to transform it to reduced row-echelon form R. The chances are quite good that they will each perform a different sequence of elementary row operations to achieve the desired result. Let R and R′ be the reduced row-echelon matrices that our two students obtain. We claim that R = R′. Indeed, since row equivalence defines an equivalence relation, we see from Theorem 3.4 that the row spaces of R and R′ will be the same. Therefore Theorem 3.7 shows us that the rows of R must equal the rows of R′. Hence we are justified in calling the reduced row-echelon form of a matrix *the* row canonical form as mentioned earlier.

Exercises

1. In the proof of Theorem 3.4, show that Ker f = {0} for a type β operation.

2. Determine whether or not the following matrices have the same row space:

$$A = \begin{pmatrix} 1 & -2 & -1 \\ 3 & -4 & 5 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & -1 & 2 \\ 3 & 3 & -1 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & -1 & 3 \\ 2 & -1 & 10 \\ 3 & -5 & 1 \end{pmatrix} .$$

3. Show that the subspace of $\mathbb{R}^3$ spanned by the vectors $u_1 = (1, 1, -1)$, $u_2 = (2, 3, -1)$ and $u_3 = (3, 1, -5)$ is the same as the subspace spanned by the vectors $v_1 = (1, -1, -3)$, $v_2 = (3, -2, -8)$ and $v_3 = (2, 1, -3)$.

4. Determine whether or not each of the following sets of vectors is linearly independent:
   (a) $u_1 = (1, -2, 1)$, $u_2 = (2, 1, -1)$ and $u_3 = (7, -4, 1)$.
   (b) $u_1 = (1, 2, -3)$, $u_2 = (1, -3, 2)$ and $u_3 = (2, -1, 5)$.

5. (a) Suppose we are given an m x n matrix $A = (a_{ij})$, and suppose that one of the columns of A, say A^i, is a linear combination of the others. Show that under any elementary row operation resulting in a new matrix $\tilde{A}$, the column $\tilde{A}^i$ is the same linear combination of the columns of $\tilde{A}$ that A^i is of the columns of A. In other words, show that all linear relations between columns are preserved by elementary row operations.
   (b) Use this result to give another proof of Theorem 3.4.
   (c) Use this result to give another proof of Theorem 3.7.

3.4 THE RANK OF A MATRIX

It is important for the reader to realize that there is nothing special about the rows of a matrix. Everything that we have done up to this point in discussing elementary row operations could just as easily have been done with columns instead. In particular, this means that Theorems 3.4 and 3.5 are equally valid for column spaces if we apply our elementary transformations to columns instead of rows. This observation leads us to our next fundamental result.

Theorem 3.8 If $A = (a_{ij})$ is any m x n matrix over a field $\mathcal{F}$, then $\mathrm{rr}(A) = \mathrm{cr}(A)$.

Proof Let $\tilde{A}$ be the reduced row-echelon form of A. By Theorem 3.4 it is sufficient to show that $\mathrm{rr}(\tilde{A}) = \mathrm{cr}(\tilde{A})$. If $j_1 < \cdots < j_r$ are the columns containing the distinguished elements of $\tilde{A}$, then $\{A^{j_1}, \dots, A^{j_r}\}$ is a basis for the column space of $\tilde{A}$, and hence $\mathrm{cr}(\tilde{A}) = r$. (In fact, these columns are just the first r standard basis vectors in $\mathcal{F}^n$.) But from the corollary to Theorem 3.5, we see that rows $\tilde{A}_1, \dots, \tilde{A}_r$ form a basis for the row space of $\tilde{A}$, and thus $\mathrm{rr}(\tilde{A}) = r$ also. ∎

In view of this result, we define the **rank** r(A) of a matrix A as

$$r(A) = rr(A) = cr(A) \;.$$

Our next theorem forms the basis for a practical method of finding the rank of a matrix.

Theorem 3.9 If A is any matrix, then r(A) is equal to the number of nonzero rows in the (reduced) row-echelon matrix row equivalent to A. (Alternatively, r(A) is the number of nonzero columns in the (reduced) column-echelon matrix column equivalent to A.)

Proof Noting that the number of nonzero rows in the row-echelon form is the same as the number of nonzero rows in the reduced row-echelon form, we see that this theorem follows directly from the corollary to Theorem 3.5. ∎

If A is an n x n matrix such that $a_{ij} = 0$ for $i \neq j$ and $a_{ii} = 1$, then we say that A is the **identity matrix** of size n and write this matrix as I_n. Since the size is usually understood, we will generally simply write I. If $I = (I_{ij})$, then another useful way of writing this is in terms of the Kronecker delta as $I_{ij} = \delta_{ij}$. Written out, I has the form

$$I = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} .$$

Theorem 3.10 If A is an n x n matrix of rank n, then the reduced row-echelon matrix row equivalent to A is the identity matrix I_n.

Proof This follows from the definition of a reduced row-echelon matrix and Theorem 3.9. ∎

Example 3.7 Let us find the rank of the matrix A given by

$$A = \begin{pmatrix} 1 & 2 & -3 \\ 2 & 1 & 0 \\ -2 & -1 & 3 \\ -1 & 4 & -2 \end{pmatrix} .$$

To do this, we will apply Theorem 3.9 to columns instead of rows (just for variety). Proceeding with the elementary transformations, we obtain the following sequence of matrices:

$$\begin{array}{ccc} \left(\begin{matrix} 1 & 0 & 0 \\ 2 & -3 & 6 \\ -2 & 3 & -3 \\ -1 & 6 & -5 \end{matrix}\right) \\ \begin{array}{ccc} & \uparrow & \uparrow \\ & A^2-2A^1 & A^3+3A^1 \end{array} \end{array}$$

$$\begin{array}{c} \left(\begin{matrix} 1 & 0 & 0 \\ 2 & -1 & 0 \\ -2 & 1 & 1 \\ -1 & 2 & 7/3 \end{matrix}\right) \\ \begin{array}{ccc} & \uparrow & \uparrow \\ & (1/3)A^2 & (1/3)(A^3+2A^2) \end{array} \end{array}$$

$$\begin{array}{c} \left(\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 3 & 1/3 & 7/3 \end{matrix}\right) \\ \begin{array}{ccc} & \uparrow & \uparrow \\ A^1+2A^2 & & -(A^2-A^3) \end{array} \end{array}$$

Thus the reduced column-echelon form of A has three nonzero columns, so that r(A) = cr(A) = 3. We leave it to the reader (see Exercise 3.4.1) to show that the row canonical form of A is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

and hence r(A) = cr(A) = rr(A) as it should. ∕∕

Exercises

1. Verify the row-canonical form of the matrix in Example 3.7.

2. Let A and B be arbitrary m x n matrices. Show that r(A + B) ≤ r(A) + r(B).

3. Using elementary row operations, find the rank of each of the following matrices:

$$(a)\ \begin{pmatrix} 1 & 3 & 1 & -2 & -3 \\ 1 & 4 & 3 & -1 & -4 \\ 2 & 3 & -4 & -7 & -3 \\ 3 & 8 & 1 & -7 & -8 \end{pmatrix} \qquad (b)\ \begin{pmatrix} 1 & 2 & -3 \\ 2 & 1 & 0 \\ -2 & -1 & 3 \\ -1 & 4 & -2 \end{pmatrix}$$

$$(c)\ \begin{pmatrix} 1 & 3 \\ 0 & -2 \\ 5 & -1 \\ -2 & 3 \end{pmatrix} \qquad (d)\ \begin{pmatrix} 5 & -1 & 1 \\ 2 & 1 & -2 \\ 0 & -7 & 12 \end{pmatrix}$$

4. Repeat the previous problem using elementary column operations.

3.5 SOLUTIONS TO SYSTEMS OF LINEAR EQUATIONS

We now apply the results of the previous section to the determination of some general characteristics of the solution set to systems of linear equations. We will have more to say on this subject after we have discussed determinants in the next chapter.

To begin with, a system of linear equations of the form

$$\sum_{j=1}^{n} a_{ij}x_j = 0, \qquad i = 1, \dots, m$$

is called a **homogeneous system** of m linear equations in n unknowns. It is obvious that choosing $x_1 = x_2 = \cdots = x_n = 0$ will satisfy this system, but this is not a very interesting solution. It is called the **trivial** (or **zero**) **solution**. Any other solution, if it exists, is referred to as a **nontrivial solution**.

A more general type of system of linear equations is of the form

$$\sum_{j=1}^{n} a_{ij}x_j = y_i, \qquad i = 1, \dots, m$$

where each y_i is a given scalar. This is then called a **nonhomogeneous system** of linear equations. Let us define the column vector

$$Y = (y_1, \dots, y_m) \in \mathcal{F}^m \;.$$

From our discussion in the proof of Theorem 3.4, we see that $a_{ij}x_j$ is just x_j times the i*th* component of the j*th* column $A^j \in \mathcal{F}^m$. Thus our system of nonhomogeneous equations may be written in the form

$$\sum_{j=1}^{n} A^j x_j = x_1\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + x_2\begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} + \cdots + x_n\begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} = Y$$

where this vector equation is to be interpreted in terms of its components. (In the next section, we shall see how to write this as a product of matrices.) It should also be obvious that a homogeneous system may be written in this notation as

$$\sum_{j=1}^{n} A^j x_j = 0 \;\;.$$

Let us now look at some elementary properties of the solution set of a homogeneous system of equations.

Theorem 3.11 The solution set S of a homogeneous system of m equations in n unknowns is a subspace of $\mathcal{F}^n$.

Proof Let us write our system as $\sum_j a_{ij}x_j = 0$. We first note that $S \neq \varnothing$ since $(0, \dots, 0) \in \mathcal{F}^n$ is the trivial solution of our system. If $u = (u_1, \dots, u_n) \in \mathcal{F}^n$ and $v = (v_1, \dots, v_n) \in \mathcal{F}^n$ are both solutions, then

$$\textstyle\sum_j a_{ij}(u_j + v_j) = \sum_j a_{ij}u_j + \sum_j a_{ij}v_j = 0$$

so that $u + v \in S$. Finally, if $c \in \mathcal{F}$ then we also have

$$\textstyle\sum_j a_{ij}(cu_j) = c\sum_j a_{ij}u_j = 0$$

so that $cu \in S$. ∎

If we look back at Example 3.4, we see that a system of m equations in n > m unknowns will necessarily result in a nonunique, and hence nontrivial, solution. The formal statement of this fact is contained in our next theorem.

Theorem 3.12 Let a homogeneous system of m equations in n unknowns have the m x n matrix of coefficients A. Then the system has a nontrivial solution if and only if r(A) < n.

Proof By writing the system in the form $\sum_j x_j A^j = 0$, it is clear that a nontrivial solution exists if and only if the n column vectors $A^j \in \mathcal{F}^m$ are linearly dependent. Since the rank of A is equal to the dimension of its column space, we must therefore have r(A) < n. ∎

It should now be clear that if an n x n (i.e., square) matrix of coefficients A (of a homogeneous system) has rank equal to n, then the only solution will be the trivial solution since reducing the augmented matrix (which then has the last column equal to the zero vector) to reduced row-echelon form will result in each variable being set equal to zero (see Theorem 3.10).

Theorem 3.13 Let a homogeneous system of linear equations in n unknowns have a matrix of coefficients A. Then the solution set S of this system is a subspace of $\mathcal{F}^n$ with dimension n - r(A).

Proof Assume that S is a nontrivial solution set, so that by Theorem 3.12 we have r(A) < n. Assume also that the unknowns $x_1, \dots, x_n$ have been ordered in such a way that the first k = r(A) columns of A span the column space (this is guaranteed by Theorem 3.4). Then the remaining columns $A^{k+1}, \dots, A^n$ may be written as

$$A^i = \sum_{j=1}^{k} b_{ij} A^j, \qquad i = k+1, \dots, n$$

and where each $b_{ij} \in \mathcal{F}$. If we define $b_{ii} = -1$ and $b_{ij} = 0$ for $j \neq i$ and $j > k$, then we may write this as

$$\sum_{j=1}^{n} b_{ij} A^j = 0, \qquad i = k+1, \dots, n$$

(note the upper limit on this sum differs from the previous equation). Next we observe that the solution set S consists of all vectors $x \in \mathcal{F}^n$ such that

$$\sum_{j=1}^{n} x_j A^j = 0$$

and hence in particular, the n - k vectors

$$b^{(i)} = (b_{i1}, \dots, b_{in})$$

for each i = k + 1, . . . , n must belong to S. We show that they in fact form a basis for S, which is then of dimension n - k.

To see this, we first write out each of the $b^{(i)}$:

$$\begin{aligned} b^{(k+1)} &= (b_{k+1\,1}, \dots , b_{k+1\,k}, -1, 0, 0, \dots , 0)\\ b^{(k+2)} &= (b_{k+2\,1}, \dots , b_{k+2\,k}, 0, -1, 0, \dots , 0)\\ &\vdots\\ b^{(n)} &= (b_{n1}, \dots , b_{nk}, 0, 0, \dots , 0, -1)\ . \end{aligned}$$

Hence for any set $\{c_i\}$ of n - k scalars we have

$$\sum_{i=k+1}^{n} c_i b^{(i)} = \left(\sum_{i=k+1}^{n} c_i b_{i1}, \dots , \sum_{i=k+1}^{n} c_i b_{in}, -c_{k+1}, \dots , -c_n \right)$$

and therefore

$$\sum_{i=k+1}^{n} c_i b^{(i)} = 0$$

if and only if $c_{k+1} = \cdots = c_n = 0$. This shows that the $b^{(i)}$ are linearly independent. (This should have been obvious from their form shown above.)

Now suppose that $d = (d_1, \dots , d_n)$ is any solution of

$$\sum_{j=1}^{n} x_j A^j = 0\ .$$

Since S is a vector space (Theorem 3.11), any linear combination of solutions is a solution, and hence the vector

$$y = d + \sum_{i=k+1}^{n} d_i b^{(i)}$$

must also be a solution. In particular, writing out each component of this expression shows that

$$y_j = d_j + \sum_{i=k+1}^{n} d_i b_{ij}$$

and hence the definition of the b_{ij} shows that $y = (y_1, \dots , y_k, 0, \dots , 0)$ for some set of scalars y_i. Therefore, we have

$$0 = \sum_{j=1}^{n} y_j A^j = \sum_{j=1}^{k} y_j A^j$$

and since $\{A^1, \dots , A^k\}$ is linearly independent, this implies that $y_j = 0$ for each j = 1, . . . , k. Hence y = 0 so that

$$d = -\sum_{i=k+1}^{n} d_i b^{(i)}$$

and we see that any solution may be expressed as a linear combination of the $b^{(i)}$.

Since the $b^{(i)}$ are linearly independent and we just showed that they span S, they must form a basis for S. ∎

Suppose that we have a homogeneous system of m equations in $n > m$ unknowns, and suppose that the coefficient matrix A is in row-echelon form and has rank m. Then each of the m successive equations contains fewer and fewer unknowns, and since there are more unknowns than equations, there will be $n - m = n - r(A)$ unknowns that do not appear as the first entry in any of the rows of A. These $n - r(A)$ unknowns are called **free variables**. We may arbitrarily assign any value we please to the free variables to obtain a solution of the system.

Let the free variables of our system be $x_{i_1}, \dots, x_{i_k}$ where $k = n - m = n - r(A)$, and let v_s be the solution vector obtained by setting x_{i_s} equal to 1 and each of the remaining free variables equal to 0. (This is essentially what was done in the proof of Theorem 3.13.) We claim that $v_1, \dots, v_k$ are linearly independent and hence form a basis for the solution space of the (homogeneous) system (which is of dimension $n - r(A)$ by Theorem 3.13).

To see this, we basically follow the proof of Theorem 3.13 and let B be the k x n matrix whose rows consist of the solution vectors v_s. For each s, our construction is such that we have $x_{i_s} = 1$ and $x_{i_r} = 0$ for $r \neq s$ (and the remaining $m = n - k$ unknowns are in general nonzero). In other words, the solution vector v_s has a 1 in the position of x_{i_s}, while for $r \neq s$ the vector v_r has a 0 in this same position. This means that each of the k columns corresponding to the free variables in the matrix B contains a single 1 and the rest zeros. We now interchange column 1 and column i_1, then column 2 and column $i_2, \dots,$ and finally column k and column i_k. This yields the matrix

$$C = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & b_{1\,k+1} & \cdots & b_{1n} \\ 0 & 1 & 0 & \cdots & 0 & 0 & b_{2\,k+1} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & & 0 & 1 & b_{k\,k+1} & \cdots & b_{kn} \end{pmatrix}$$

where the entries $b_{i\,k+1}, \dots, b_{in}$ are the values of the remaining m unknowns in the solution vector v_i. Since the matrix C is in row-echelon form, its rows are independent and hence $r(C) = k$. However, C is column-equivalent to B, and therefore $r(B) = k$ also (by Theorem 3.4 applied to columns). But the rows of B consist precisely of the k solution vectors v_s, and thus these solution vectors must be independent as claimed.

Example 3.8 Consider the homogeneous system of linear equations

$$\begin{aligned} x + 2y - 4z + 3w - \ \ t &= 0 \\ x + 2y - 2z + 2w + \ \ t &= 0 \\ 2x + 4y - 2z + 3w + 4t &= 0 \end{aligned}$$

If we reduce this system to row-echelon form, we obtain

$$\begin{aligned} x + 2y - 4z + 3w - \ \ t &= 0 \\ 2z - \ \ w + 2t &= 0 \end{aligned} \tag{*}$$

It is obvious that the rank of the matrix of coefficients is 2, and hence the dimension of the solution space is 5 - 2 = 3. The free variables are clearly y, w and t. The solution vectors v_s are obtained by choosing (y = 1, w = 0, t = 0), (y = 0, w = 1, t = 0) and (y = 0, w = 0, t = 1). Using each of the these in the system (*), we obtain the solutions

$$\begin{aligned} v_1 &= (-2, 1, 0, 0, 0) \\ v_2 &= (-1, 0, 1/2, 1, 0) \\ v_3 &= (-3, 0, -1, 0, 1) \end{aligned}$$

Thus the vectors v_1, v_2 and v_3 form a basis for the solution space of the homogeneous system. ∕∕

We emphasize that the corollary to Theorem 3.4 shows us that the solution set of a homogeneous system of equations is unchanged by elementary row operations. It is this fact that allows us to proceed as we did in Example 3.8.

We now turn our attention to the solutions of a nonhomogeneous system of equations $\sum_j a_{ij}x_j = y_i$.

Theorem 3.14 Let a nonhomogeneous system of linear equations have matrix of coefficients A. Then the system has a solution if and only if r(A) = r(aug A).

Proof Let c = $(c_1, \dots, c_n)$ be a solution of $\sum_j a_{ij}x_j = y_i$. Then writing this as

$$\sum\nolimits_j c_j A^j = Y$$

shows us that Y is in the column space of A, and hence

$$r(\text{aug } A) = cr(\text{aug } A) = cr(A) = r(A) \ .$$

Conversely, if cr(aug A) = r(aug A) = r(A) = cr(A), then Y is in the column space of A, and hence $Y = \sum c_j A^j$ for some set of scalars c_j . But then the vector $c = (c_1, \dots, c_n)$ is a solution since it obviously satisfies $\sum_j a_{ij} x_j = y_i$. ∎

Using Theorem 3.13, it is easy to describe the general solution to a nonhomogeneous system of equations.

Theorem 3.15 Let

$$\sum_{j=1}^{n} a_{ij} x_j = y_j$$

be a system of nonhomogeneous linear equations. If $u = (u_1, \dots, u_n) \in \mathcal{F}^n$ is a solution of this system, and if S is the solution space of the associated homogeneous system, then the set

$$u + S = \{u + v: v \in S\}$$

is the solution set of the nonhomogeneous system.

Proof If $w = (w_1, \dots, w_n) \in \mathcal{F}^n$ is any other solution of $\sum_j a_{ij} x_j = y_i$, then

$$\sum_j a_{ij}(w_j - u_j) = \sum_j a_{ij} w_j - \sum_j a_{ij} u_j = y_i - y_i = 0$$

so that $w - u \in S$, and hence $w = u + v$ for some $v \in S$. Conversely, if $v \in S$ then

$$\sum_j a_{ij}(u_j + v_j) = \sum_j a_{ij} u_j + \sum_j a_{ij} v_j = y_j + 0 = y_j$$

so that u + v is a solution of the nonhomogeneous system. ∎

Theorem 3.16 Let A be an n x n matrix of rank n. Then the system

$$\sum_{j=1}^{n} A^j x_j = Y$$

has a unique solution for arbitrary vectors $Y \in \mathcal{F}^n$.

Proof Since $Y = \sum A^j x_j$, we see that $Y \in \mathcal{F}^n$ is just a linear combination of the columns of A. Since r(A) = n, it follows that the columns of A are linearly independent and hence form a basis for $\mathcal{F}^n$. But then any $Y \in \mathcal{F}^n$ has a unique expansion in terms of this basis (Theorem 2.4, Corollary 2) so that the vector X with components x_j must be unique. ∎

Example 3.9 Let us find the complete solution set over the real numbers of the nonhomogeneous system

$$\begin{aligned} 3x_1 + \ x_2 + \ 2x_3 + \ 4x_4 &= \ 1 \\ x_1 - \ x_2 + \ 3x_3 - \ x_4 &= \ 3 \\ x_1 + 7x_2 - 11x_3 + 13x_4 &= -13 \\ 11x_1 + \ x_2 + 12x_3 + 10x_4 &= \ 9 \end{aligned}$$

We assume that we somehow found a particular solution u = (2, 5, 1, −3) ∈ $\mathbb{R}^4$, and hence we seek the solution set S of the associated homogeneous system. The matrix of coefficients A of the homogeneous system is given by

$$A = \begin{pmatrix} 3 & 1 & 2 & 4 \\ 1 & -1 & 3 & -1 \\ 1 & 7 & -11 & 13 \\ 11 & 1 & 12 & 10 \end{pmatrix}.$$

The first thing we must do is determine r(A). Since the proof of Theorem 3.13 dealt with columns, we choose to construct a new matrix B by applying elementary column operations to A. Thus we define

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 4 & 5 & 3 \\ 7 & -20 & -25 & -15 \\ 1 & 8 & 10 & 6 \end{pmatrix}$$

where the columns of B are given in terms of those of A by $B^1 = A^2$, $B^2 = A^1 - 3A^2$, $B^3 = A^3 - 2A^2$ and $B^4 = A^4 - 4A^2$. It is obvious that B^1 and B^2 are independent, and we also note that $B^3 = (5/4)B^2$ and $B^4 = (3/4)B^2$. Then r(A) = r(B) = 2, and hence we have dim S = 4 − 2 = 2.

(An alternative method of finding r(A) is as follows. If we interchange the first two rows of A and then add a suitable multiple the new first row to eliminate the first entry in each of the remaining three rows, we obtain

$$\begin{pmatrix} 1 & -1 & 3 & -1 \\ 0 & 4 & -7 & 7 \\ 0 & 8 & -14 & 14 \\ 0 & 12 & -21 & 21 \end{pmatrix}.$$

It is now clear that the first two rows of this matrix are independent, and that the third and fourth rows are each multiples of the second. Therefore r(A) = 2 as above.)

We now follow the first part of the proof of Theorem 3.13. Observe that since r(A) = 2 and the first two columns of A are independent, we may write

$$\mathrm{A}^3 = (5/4)\mathrm{A}^1 - (7/4)\mathrm{A}^2$$

and

$$\mathrm{A}^4 = (3/4)\mathrm{A}^1 + (7/4)\mathrm{A}^2 \quad .$$

We therefore define the vectors

$$\mathrm{b}^{(3)} = (5/4, -7/4, -1, 0)$$

and

$$\mathrm{b}^{(4)} = (3/4, 7/4, 0, -1)$$

which are independent solutions of the homogeneous system and span the solution space S. Therefore the general solution set to the nonhomogeneous system is given by

$$\begin{aligned} u + S &= \{u + \alpha b^{(3)} + \beta b^{(4)}\} \\ &= \{(2, 5, 1, -3) + \alpha(5/4, -7/4, -1, 0) + \beta(3/4, 7/4, 0, 1)\} \end{aligned}$$

where $\alpha, \beta \in \mathbb{R}$ are arbitrary. ∕∕

Exercises

1. Find the dimension and a basis for the solution space of each of the following systems of linear equations over $\mathbb{R}$:

$$(a)\quad \begin{aligned} x + 4y + 2z &= 0 \\ 2x + y + 5z &= 0 \end{aligned} \qquad\qquad (b)\quad \begin{aligned} x + 3y + 2z &= 0 \\ x + 5y + z &= 0 \\ 3x + 5y + 8z &= 0 \end{aligned}$$

$$(c)\quad \begin{aligned} x + 2y + 2z - w + 3t &= 0 \\ x + 2y + 3z + w + t &= 0 \\ 3x + 6y + 8z + w + t &= 0 \end{aligned} \qquad\qquad (d)\quad \begin{aligned} x + 2y - 2z - 2w - t &= 0 \\ x + 2y - z + 3w - 2t &= 0 \\ 2x + 4y - 7z + w + t &= 0 \end{aligned}$$

2. Consider the subspaces U and V of $\mathbb{R}^4$ given by

$$U = \{(a, b, c, d) \in \mathbb{R}^4 : b + c + d = 0\}$$
$$V = \{(a, b, c, d) \in \mathbb{R}^4 : a + b = 0 \text{ and } c = 2d\} \ .$$

   (a) Find the dimension and a basis for U.
   (b) Find the dimension and a basis for V.
   (c) Find the dimension and a basis for U ∩ V.

3. Find the complete solution set of each of the following systems of linear equations over $\mathbb{R}$:

$$(a)\ \begin{aligned} 3x - y &= 7 \\ 2x + y &= 1 \end{aligned} \qquad (b)\ \begin{aligned} 2x - \ \ y + 3z &= \ 5 \\ 3x + 2y - 2z &= \ 1 \\ 7x + \qquad 4z &= 11 \end{aligned}$$

$$(c)\ \begin{aligned} 5x + 2y - \ z &= 0 \\ 3x + 5y + 3z &= 0 \\ x + 8y + 7z &= 0 \end{aligned} \qquad (d)\ \begin{aligned} x - \ y + 2z + \ w &= 3 \\ 2x + \ y - \ z - \ w &= 1 \\ 3x + \ y + \ z - 3w &= 2 \\ 3x - 2y + 6z \qquad &= 7 \end{aligned}$$

3.6 MATRIX ALGEBRA

We now introduce the elementary algebraic operations on matrices. These operations will be of the utmost importance throughout the remainder of this text. In Chapter 5 we will see how these definitions arise in a natural way from the algebra of linear transformations.

Given two m x n matrices A = (a_{ij}) and B = (b_{ij}), we define their **sum** A + B to be the matrix with entries

$$(A + B)_{ij} = a_{ij} + b_{ij}$$

obtained by adding the corresponding entries of each matrix. Note that both A and B must be of the same size. We also say that A **equals** B if $a_{ij} = b_{ij}$ for all i and j. It is obvious that

$$A + B = B + A$$

and that

$$A + (B + C) = (A + B) + C$$

for any other m x n matrix C. We also define the **zero matrix** 0 as that matrix for which A + 0 = A. In other words, $(0)_{ij} = 0$ for every i and j. Given a matrix $A = (a_{ij})$, we define its **negative** (or **additive inverse**)

$$-A = (-a_{ij})$$

such that A + (−A) = 0. Finally, for any scalar c we define the product of c and A to be the matrix

$$cA = (ca_{ij}) \ .$$

Since in general the entries a_{ij} in a matrix $A = (a_{ij})$ are independent of each other, it should now be clear that the set of all m x n matrices forms a vector space of dimension mn over a field $\mathcal{F}$ of scalars. In other words, any m x n matrix A with entries a_{ij} can be written in the form

$$A = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}E_{ij}$$

where the m x n matrix E_{ij} is defined as having a 1 in the (i, j)*th* position and 0's elsewhere, and there are clearly mn such matrices. We denote the space of all m x n matrices over the field $\mathcal{F}$ by $M_{m\mathrm{x}n}(\mathcal{F})$. The particular case of m = n defines the space $M_n(\mathcal{F})$ of all **square** matrices of size n. We will often refer to a matrix in $M_n(\mathcal{F})$ as an **n-square** matrix.

Now let $A \in M_{m\mathrm{x}n}(\mathcal{F})$ be an m x n matrix, $B \in M_{r\mathrm{x}m}(\mathcal{F})$ be an r x m matrix, and consider the two systems of linear equations

$$\sum_{j=1}^{n} a_{ij}x_j = y_i, \qquad i = 1, \dots, m$$

and

$$\sum_{j=1}^{m} b_{ij}y_j = z_i, \qquad i = 1, \dots, r$$

where $X = (x_1, \dots, x_n) \in \mathcal{F}^n$, $Y = (y_1, \dots, y_m) \in \mathcal{F}^m$ and $Z = (z_1, \dots, z_r) \in \mathcal{F}^r$. Substituting the first of these equations into the second yields

$$z_i = \Sigma_j b_{ij} y_j = \Sigma_j b_{ij} \Sigma_k a_{jk} x_k = \Sigma_k c_{ik} x_k$$

where we defined the **product** of the r x m matrix B and the m x n matrix A to be the r x n matrix C = BA whose entries are given by

$$c_{ik} = \sum_{j=1}^{m} b_{ij}a_{jk} \ .$$

Thus the (i, k)*th* entry of C = BA is given by the standard scalar product

$$(\mathrm{BA})_{\mathrm{i\,k}} = \mathrm{B_i} \bullet \mathrm{A^k}$$

of the i*th* row of B with the k*th* column of A (where both are considered as vectors in $\mathcal{F}^{\mathrm{m}}$). Note that matrix multiplication is generally not commutative, i.e., AB ≠ BA. Indeed, the product AB may not even be defined.

Example 3.10 Let A and B be given by

$$A = \begin{pmatrix} 1 & 6 & -2 \\ 3 & 4 & 5 \\ 7 & 0 & 8 \end{pmatrix} \qquad\qquad B = \begin{pmatrix} 2 & -9 \\ 6 & 1 \\ 1 & -3 \end{pmatrix} .$$

Then the product of A and B is given by

$$C = AB = \begin{pmatrix} 1 & 6 & -2 \\ 3 & 4 & 5 \\ 7 & 0 & 8 \end{pmatrix} \begin{pmatrix} 2 & -9 \\ 6 & 1 \\ 1 & -3 \end{pmatrix} = \begin{pmatrix} 1\cdot 2+6\cdot 6-2\cdot 1 & -1\cdot 9+6\cdot 1+2\cdot 3 \\ 3\cdot 2+4\cdot 6+5\cdot 1 & -3\cdot 9+4\cdot 1-5\cdot 3 \\ 7\cdot 2+0\cdot 6+8\cdot 1 & -7\cdot 9+0\cdot 1-8\cdot 3 \end{pmatrix}$$

$$= \begin{pmatrix} 36 & 3 \\ 35 & -38 \\ 22 & -87 \end{pmatrix} .$$

Note that it makes no sense to evaluate the product BA.

It is also easy to see that if we have the matrices

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

then

$$AB = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}$$

while

$$BA = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} \ne AB \ . \ /\!/$$

Example 3.11 Two other special cases of matrix multiplication are worth explicitly mentioning. Let $\mathrm{X} \in \mathcal{F}^{\mathrm{n}}$ be the column vector

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \ .$$

If A is an m x n matrix, we may consider X to be an n x 1 matrix and form the product AX:

$$AX = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix} = \begin{pmatrix} A_1 \bullet X \\ \vdots \\ A_m \bullet X \end{pmatrix} \ .$$

As expected, the product AX is an m x 1 matrix with entries given by the standard scalar product $A_i \bullet X$ in $\mathcal{F}^n$ of the i*th* row of A with the vector X. Note that this may also be written in the form

$$AX = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} x_1 + \cdots + \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} x_n$$

which clearly shows that AX is just a linear combination of the columns of A.

Now let $Y \in \mathcal{F}^m$ be the row vector $Y = (y_1, \ldots, y_m)$. If we view this as a 1 x m matrix, then we may form the 1 x n matrix product YA given by

$$\begin{aligned} YA &= (y_1, \ldots, y_m) \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \\ &= (y_1 a_{11} + \cdots + y_m a_{m1}, \ldots, y_1 a_{1n} + \cdots + y_m a_{mn}) \\ &= (Y \bullet A^1, \ldots, Y \bullet A^n) \ . \end{aligned}$$

This again yields the expected form of the product with entries $Y \bullet A^i$. ∕∕

This example suggests the following commonly used notation for systems of linear equations. Consider the system

$$\sum_{j=1}^{n} a_{ij} x_j = y_i$$

where $A = (a_{ij})$ is an m x n matrix. Suppose that we define the column vectors

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{F}^n \quad \text{and} \quad Y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \in \mathcal{F}^m \ .$$

If we consider X to be an n x 1 matrix and Y to be an m x 1 matrix, then we may write this system in matrix notation as

$$AX = Y \ .$$

Note that the *ith* row vector of A is $A_i = (a_{i1}, \ldots, a_{in})$ so that the expression $\sum_j a_{ij} x_j = y_i$ may be written as the standard scalar product

$$A_i \bullet X = y_i \ .$$

We leave it to the reader to show that if A is an n x n matrix, then

$$A I_n = I_n A = A \ .$$

Even if A and B are both square matrices (i.e., matrices of the form m x m), the product AB will not generally be the same as BA unless A and B are diagonal matrices (see Exercise 3.6.4). However, we do have the following.

Theorem 3.17 For matrices of proper size (so that these operations are defined), we have:

(a) (AB)C = A(BC) (associative law).
(b) A(B + C) = AB + AC (left distributive law).
(c) (B + C)A = BA + CA (right distributive law).
(d) k(AB) = (kA)B = A(kB) for any scalar k.

Proof (a)
$$\begin{aligned}[(AB)C]_{ij} &= \Sigma_k (AB)_{ik} c_{kj} = \Sigma_{r,\,k} (a_{ir} b_{rk}) c_{kj} = \Sigma_{r,\,k} a_{ir} (b_{rk} c_{kj}) \\ &= \Sigma_r a_{ir} (BC)_{rj} = [A(BC)]_{ij} \ .\end{aligned}$$

(b)
$$\begin{aligned}[A(B+C)]_{ij} &= \Sigma_k a_{ik} (B+C)_{kj} = \Sigma_k a_{ik} (b_{kj} + c_{kj}) \\ &= \Sigma_k a_{ik} b_{kj} + \Sigma_k a_{ik} c_{kj} = (AB)_{ij} + (AC)_{ij} \\ &= [(AB) + (AC)]_{ij} \ .\end{aligned}$$

(c) Left to the reader (Exercise 3.6.1).
(d) Left to the reader (Exercise 3.6.1). ∎

Given a matrix $A = (a_{ij})$, we define the **transpose** of A, denoted by $A^T = (a^T{}_{ij})$ to be the matrix with entries given by $a^T{}_{ij} = a_{ji}$. In other words, if A is an m x n matrix, then A^T is an n x m matrix whose columns are just the rows of A. Note in particular that a column vector is just the transpose of a row vector.

Example 3.12 If A is given by

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

then A^T is given by

$$\begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} . \;//$$

Theorem 3.18 The transpose has the following properties:

(a) $(A + B)^T = A^T + B^T$.
(b) $(A^T)^T = A$.
(c) $(cA)^T = cA^T$ for any scalar c.
(d) $(AB)^T = B^T A^T$.

Proof (a) $[(A + B)^T]_{ij} = [(A + B)]_{ji} = a_{ji} + b_{ji} = a^T{}_{ij} + b^T{}_{ij} = (A^T + B^T)_{ij}$.
(b) $(A^T)^T{}_{ij} = (A^T)_{ji} = a_{ij} = (A)_{ij}$.
(c) $(cA)^T{}_{ij} = (cA)_{ji} = ca_{ji} = c(A^T)_{ij}$.
(d) $(AB)^T{}_{ij} = (AB)_{ji} = \sum_k a_{jk}b_{ki} = \sum_k b^T{}_{ik}a^T{}_{kj} = (B^T A^T)_{ij}$. ∎

We now wish to relate this algebra to our previous results dealing with the rank of a matrix. Before doing so, let us first make some elementary observations dealing with the rows and columns of a matrix product. Assume that $A \in M_{m\mathrm{x}n}(\mathcal{F})$ and $B \in M_{n\mathrm{x}r}(\mathcal{F})$ so that the product AB is defined. Since the (i, j)*th* entry of AB is given by $(AB)_{ij} = \sum_k a_{ik}b_{kj}$, we see that the i*th* row of AB is given by a linear combination of the rows of B:

$$(AB)_i = (\textstyle\sum_k a_{ik}b_{k1}, \dots, \sum_k a_{ik}b_{kr}) = \sum_k a_{ik}(b_{k1}, \dots, b_{kr}) = \sum_k a_{ik}B_k \;.$$

Another way to write this is to observe that

$$\begin{aligned}(AB)_i &= (\Sigma_k a_{ik}b_{k1}, \dots, \Sigma_k a_{ik}b_{kr})\\ &= (a_{i1}, \dots, a_{in})\begin{pmatrix} b_{11} & \cdots & b_{1r}\\ \vdots & & \vdots\\ b_{n1} & \cdots & b_{nr}\end{pmatrix} = A_iB \ .\end{aligned}$$

Similarly, for the columns of a product we find that the *jth* column of AB is a linear combination of the columns of A:

$$(AB)^j = \begin{pmatrix} \Sigma_k a_{1k}b_{kj}\\ \vdots\\ \Sigma_k a_{mk}b_{kj}\end{pmatrix} = \sum_{k=1}^{n}\begin{pmatrix} a_{1k}\\ \vdots\\ a_{mk}\end{pmatrix} b_{kj} = \sum_{k=1}^{n} A^k b_{kj}$$

and

$$(AB)^j = \begin{pmatrix} \Sigma_k a_{1k}b_{kj}\\ \vdots\\ \Sigma_k a_{mk}b_{kj}\end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n}\\ \vdots & & \vdots\\ a_{m1} & \cdots & a_{mn}\end{pmatrix}\begin{pmatrix} b_{1j}\\ \vdots\\ b_{nj}\end{pmatrix} = AB^j \ .$$

These formulas will be quite useful to us in several of the following theorems.

Theorem 3.19 For any matrix A we have $r(A^T) = r(A)$.

Proof This is Exercise 3.6.2. ∎

Theorem 3.20 If A and B are any matrices for which the product AB is defined, then the row space of AB is a subspace of the row space of B, and the column space of AB is a subspace of the column space of A.

Proof Using $(AB)_i = \Sigma_k a_{ik} B_k$, we see that the *ith* row of AB is in the space spanned by the rows of B, and hence the row space of AB is a subspace of the row space of B.

Now note that the column space of AB is just the row space of $(AB)^T = B^T A^T$, which is a subspace of the row space of A^T by the first part of the theorem. But the row space of A^T is just the column space of A. ∎

Corollary $r(AB) \le \min\{r(A), r(B)\}$.

Proof Let V_A be the row space of A, and let W_A be the column space of A. Then

$$r(AB) = \dim V_{AB} \le \dim V_B = r(B)$$

while

$$r(AB) = \dim W_{AB} \le \dim W_A = r(A)\ . \ ∎$$

Exercises

1. Complete the proof of Theorem 3.17.

2. Prove Theorem 3.19.

3. Let A be any m x n matrix and let X be any n x 1 matrix, both with entries in $\mathcal{F}$. Define the mapping $f : \mathcal{F}^n \rightarrow \mathcal{F}^m$ by $f(X) = AX$.
(a) Show that f is a linear transformation (i.e., a vector space homomorphism).
(b) Define $\text{Im}\, f = \{AX: X \in \mathcal{F}^n\}$. Show that Im f is a subspace of $\mathcal{F}^m$.
(c) Let U be the column space of A. Show that Im f = U. [*Hint*: Use Example 3.11 to show that $\text{Im}\, f \subset U$. Next use the equation $(AI)^j = AI^j$ to show that $U \subset \text{Im}\, f$.]
(d) Let N denote the solution space to the system AX = 0. In other words, $N = \{X \in \mathcal{F}^n: AX = 0\}$. (N is usually called the **null space** of A.) Show that

$$\dim N + \dim U = n\ .$$

[*Hint*: Suppose dim N = r, and extend a basis $\{x_1, \dots, x_r\}$ for N to a basis $\{x_i\}$ for $\mathcal{F}^n$. Show that U is spanned by the vectors $Ax_{r+1}, \dots, Ax_n$, and then that these vectors are linearly independent. Note that this exercise is really just another proof of Theorem 3.13.]

4. A matrix of the form

$$\begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ 0 & a_{22} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{pmatrix}$$

is called a **diagonal** matrix. In other words, $A = (a_{ij})$ is diagonal if $a_{ij} = 0$ for $i \ne j$. If A and B are both square matrices, we may define the **commutator** [A, B] of A and B to be the matrix [A, B] = AB - BA. If [A, B] = 0, we say that A and B **commute**.
(a) Show that any diagonal matrices A and B commute.

(b) Prove that the only n x n matrices which commute with every n x n diagonal matrix are diagonal matrices.

5. Given the matrices
6.

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 0 \\ -3 & 4 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & -2 & -5 \\ 3 & 4 & 0 \end{pmatrix}$$

compute the following:
(a) AB.
(b) BA.
(c) AA^T.
(d) A^TA.
(e) Verify that $(AB)^T = B^TA^T$.

6. Consider the matrix $A \in M_n(\mathcal{F})$ given by

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} .$$

Thus A has zero entries everywhere except on the **superdiagonal** where the entries are 1's. Let $A^2 = AA$, $A^3 = AAA$, and so on. Show that $A^n = 0$ but $A^{n-1} \neq 0$.

7. Given a matrix $A = (a_{ij}) \in M_n(\mathcal{F})$, the sum of the diagonal elements of A is called the **trace** of A, and is denoted by Tr A. Thus

$$\operatorname{Tr} A = \sum_{i=1}^{n} a_{ii} \quad .$$

(a) Prove that Tr(A + B) = Tr A + Tr B and that Tr(αA) = α(Tr A) for any scalar α.
(b) Prove that Tr(AB) = Tr(BA).

8. (a) Prove that it is impossible to find matrices $A, B \in M_n(\mathbb{R})$ such that their commutator $[A, B] = AB - BA$ is equal to 1.

(b) Let $\mathcal{F}$ be a field of characteristic 2 (i.e., a field in which 1 + 1 = 0; see Exercise 1.5.17). Prove that it is possible to find matrices A, B ∈ $M_2(\mathcal{F})$ such that [A, B] = 1.

9. A matrix A = (a_{ij}) is said to be **upper-triangular** if $a_{ij} = 0$ for i > j. In other words, every entry of A below the main diagonal is zero. Similarly, A is said to be **lower-triangular** if $a_{ij} = 0$ for i < j. Prove that the product of upper (lower) triangular matrices is an upper (lower) triangular matrix.

10. Consider the so-called **Pauli spin matrices**

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and define the permutation symbol ε_{ijk} by

$$\varepsilon_{ijk} = \begin{cases} 1 & \text{if } (i,\ j,\ k) \text{ is an even permutation of } (1, 2, 3) \\ -1 & \text{if } (i,\ j,\ k) \text{ is an odd permutation of } (1, 2, 3) \\ 0 & \text{if any two indices are the same} \end{cases} .$$

The **commutator** of two matrices A, B ∈ $M_n(\mathcal{F})$ is defined by [A, B] = AB − BA, and the **anticommutator** is given by $[A, B]_+ = AB + BA$.

(a) Show that $[\sigma_i, \sigma_j] = 2i \sum_k \varepsilon_{ijk} \sigma_k$. In other words, show that $\sigma_i\sigma_j = i\sigma_k$ where (i, j, k) is an even permutation of (1, 2, 3).
(b) Show that $[\sigma_i, \sigma_j]_+ = 2I\delta_{ij}$.
(c) Using part (a), show that Tr $\sigma_i = 0$.
(d) For notational simplicity, define $\sigma_0 = I$. Show that $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ forms a basis for $M_2(\mathbb{C})$. [*Hint*: Show that $\mathrm{Tr}(\sigma_\alpha \sigma_\beta) = 2\delta_{\alpha\beta}$ where $0 \le \alpha, \beta \le 3$. Use this to show that $\{\sigma_\alpha\}$ is linearly independent.]
(e) According to part (d), any X ∈ $M_2(\mathbb{C})$ may be written in the form $X = \sum_\alpha x_\alpha \sigma_\alpha$. How would you find the coefficients x_α?
(f) Show that $\langle \sigma_\alpha, \sigma_\beta \rangle = (1/2)\mathrm{Tr}(\sigma_\alpha \sigma_\beta)$ defines an inner product on $M_2(\mathbb{C})$.
(g) Show that any matrix X ∈ $M_2(\mathbb{C})$ that commutes with all of the σ_i (i.e., $[X, \sigma_i] = 0$ for each i = 1, 2, 3) must be a multiple of the identity matrix.

11. A square matrix S is said to be **symmetric** if $S^T = S$, and a square matrix A is said to be **skewsymmetric** (or **antisymmetric**) if $A^T = -A$. (We continue to assume as usual that $\mathcal{F}$ is not of characteristic 2.)
   (a) Show that $S \neq 0$ and A are linearly independent in $M_n(\mathcal{F})$.
   (b) What is the dimension of the space of all n x n symmetric matrices?
   (c) What is the dimension of the space of all n x n antisymmetric matrices?

12. Find a basis $\{A_i\}$ for the space $M_n(\mathcal{F})$ that consists only of matrices with the property that $A_i^2 = A_i$ (such matrices are called **idempotent** or **projections**). [*Hint*: The matrices

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}\quad\begin{pmatrix}1&1\\0&0\end{pmatrix}\quad\begin{pmatrix}0&0\\1&0\end{pmatrix}\quad\begin{pmatrix}0&0\\1&1\end{pmatrix}$$

will work in the particular case of $M_2(\mathcal{F})$.]

13. Show that it is impossible to find a basis for $M_n(\mathcal{F})$ such that every pair of matrices in the basis commute with each other.

14. (a) Show that the set of all nonsingular n x n matrices forms a spanning set for $M_n(\mathcal{F})$. Exhibit a basis of such matrices.
   (b) Repeat part (a) with the set of all singular matrices.

15. Show that the set of all matrices of the form AB − BA do not span $M_n(\mathcal{F})$. [*Hint*: Use the trace.]

16. Is it possible to span $M_n(\mathcal{F})$ using powers of a single matrix A? In other words, can $\{I_n , A, A^2, \ldots , A^n, \ldots\}$ span $M_n(\mathcal{F})$? [*Hint*: Consider Exercise 4 above.]

3.7 INVERTIBLE MATRICES

We say that a matrix $A \in M_n(\mathcal{F})$ is **nonsingular** if $r(A) = n$, and **singular** if $r(A) < n$. Given a matrix $A \in M_n(\mathcal{F})$, if there exists a matrix $B \in M_n(\mathcal{F})$ such that $AB = BA = I_n$, then B is called an **inverse** of A, and A is said to be **invertible**.

Technically, a matrix B is called a **left inverse** of A if $BA = I$, and a matrix B' is a **right inverse** of A if $AB' = I$. Then, if $AB = BA = I$, we say that B is a **two-sided inverse** of A, and A is then said to be **invertible**.

Furthermore, if A has a left inverse B and a right inverse B′, then it is easy to see that B = B′ since B = BI = B(AB′) = (BA)B′ = IB′ = B′. We shall now show that if B is either a left or a right inverse of A, then A is invertible.

Theorem 3.21 A matrix $A \in M_n(\mathcal{F})$ has a right (left) inverse if and only if A is nonsingular. This right (left) inverse is also a left (right) inverse, and hence is an inverse of A.

Proof Suppose A has a right inverse B. Then $AB = I_n$ so that $r(AB) = r(I_n)$. Since $r(I_n)$ is clearly equal to n (Theorem 3.9), we see that $r(AB) = n$. But then from the corollary to Theorem 3.20 and the fact that both A and B are n x n matrices (so that $r(A) \le n$ and $r(B) \le n$), it follows that $r(A) = r(B) = n$, and hence A is nonsingular.

Now suppose that A is nonsingular so that $r(A) = n$. If we let E^j be the *jth* column of the identity matrix I_n, then for each j = 1, . . . , n the system of equations

$$\sum_{i=1}^{n} A^i x_i = AX = E^j$$

has a unique solution which we denote by $X = B^j$ (Theorem 3.16). Now let B be the matrix with columns B^j. Then the *jth* column of AB is given by

$$(AB)^j = AB^j = E^j$$

and hence $AB = I_n$. It remains to be shown that $BA = I_n$. To see this, note that $r(A^T) = r(A) = n$ (Theorem 3.19) so that A^T is nonsingular also. Hence applying the same argument shows there exists a unique n x n matrix C^T such that $A^T C^T = I_n$. Since $(CA)^T = A^T C^T$ and $I_n{}^T = I_n$, this is the same as $CA = I_n$. We now recall that it was shown prior to the theorem that if A has both a left and a right inverse, then they are the same. Therefore B = C so that BA = AB = I_n, and hence B is an inverse of A. Clearly, the proof remains valid if “right” is replaced by “left” throughout. ∎

Corollary 1 A matrix $A \in M_n(\mathcal{F})$ is nonsingular if and only if it has an inverse. Furthermore, this inverse is unique.

Proof As we saw above, if B and C are both inverses of A, then B = BI = B(AC) = (BA)C = IC = C. ∎

In view of this corollary, the unique inverse to a matrix A will be denoted by A^{-1} from now on.

Corollary 2 If A is an n x n nonsingular matrix, then A^{-1} is nonsingular and $(A^{-1})^{-1} = A$.

Proof If A is nonsingular, then (by Theorem 3.21) A^{-1} exists so that $A^{-1}A = AA^{-1} = I$. But this means that $(A^{-1})^{-1}$ exists and is equal to A, and hence A^{-1} is also nonsingular. ∎

Corollary 3 If A and B are nonsingular then so is AB, and $(AB)^{-1} = B^{-1} A^{-1}$.

Proof The fact that A and B are nonsingular means that A^{-1} and B^{-1} exist. We therefore see that

$$(B^{-1}A^{-1})(AB) = B^{-1}IB = B^{-1}B = I$$

and similarly $(AB)(B^{-1}A^{-1}) = I$. It then follows that $B^{-1} A^{-1} = (AB)^{-1}$. Since we have now shown that AB has an inverse, Theorem 3.21 tells us that AB must be nonsingular. ∎

Corollary 4 If A is nonsingular then so is A^T, and $(A^T)^{-1} = (A^{-1})^T$.

Proof That A^T is nonsingular is a direct consequence of Theorem 3.19. Next we observe that

$$(A^{-1})^T A^T = (AA^{-1})^T = I^T = I$$

so that the uniqueness of the inverse tells us that $(A^T)^{-1} = (A^{-1})^T$. Note this also shows that A^T is nonsingular. ∎

Corollary 5 A system of n linear equations in n unknowns has a unique solution if and only if its matrix of coefficients is nonsingular.

Proof Consider the system AX = Y. If A is nonsingular, then a unique A^{-1} exists, and therefore we have $X = A^{-1}Y$ as the unique solution. (Note that this is essentially the content of Theorem 3.16.)

Conversely, if this system has a unique solution, then the solution space of the associated homogeneous system must have dimension 0 (Theorem 3.15). Then Theorem 3.13 shows that we must have r(A) = n, and hence A is nonsingular. ∎

A major problem that we have not yet discussed is how to actually find the inverse of a matrix. One method involves the use of determinants as we will see in the next chapter. However, let us show another approach based on the fact that a nonsingular matrix is row-equivalent to the identity matrix

(Theorem 3.10). This method has the advantage that it is algorithmic, and hence is easily implemented on a computer.

Since the j*th* column of a product AB is AB^j, we see that considering the particular case of $AA^{-1} = I$ leads to

$$(AA^{-1})^j = A(A^{-1})^j = E^j$$

where E^j is the j*th* column of I. What we now have is the nonhomogeneous system

$$AX = Y$$

(or $\sum_j a_{ij}x_j = y_i$) where $X = (A^{-1})^j$ and $Y = E^j$. As we saw in Section 3.2, we may solve for the vector X by reducing the augmented matrix to reduced row-echelon form. For the particular case of j = 1 we have

$$\text{aug } A = \begin{pmatrix} a_{11} & \cdots & a_{1n} & 1 \\ a_{21} & \cdots & a_{2n} & 0 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 \end{pmatrix}$$

and hence the reduced form will be

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & c_{11} \\ 0 & 1 & 0 & \cdots & 0 & c_{21} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & c_{n1} \end{pmatrix}$$

for some set of scalars c_{ij}. This means that the solution to the system is $x_1 = c_{11}$, $x_2 = c_{21}$, . . . , $x_n = c_{n1}$. But $X = (A^{-1})^1$ = the first column of A^{-1}, and therefore this last matrix may be written as

$$\begin{pmatrix} 1 & \cdots & 0 & a^{-1}{}_{11} \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 1 & a^{-1}{}_{n1} \end{pmatrix} .$$

Now, for each j = 1, . . . , n the system $AX = A(A^{-1})^j = E^j$ always has the same matrix of coefficients, and only the last column of the augmented matrix depends on j. Since finding the reduced row-echelon form of the matrix of coefficients is independent of this last column, it follows that we may solve all n systems simultaneously by reducing the single matrix

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & | & 1 & \cdots & 0 \\ \vdots & & \vdots & | & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} & | & 0 & \cdots & 1 \end{pmatrix}.$$

In other words, the reduced form will be

$$\begin{pmatrix} 1 & \cdots & 0 & | & a^{-1}{}_{11} & \cdots & a^{-1}{}_{1n} \\ \vdots & & \vdots & | & \vdots & & \vdots \\ 0 & \cdots & 1 & | & a^{-1}{}_{n1} & \cdots & a^{-1}{}_{nn} \end{pmatrix}$$

where the matrix $A^{-1} = (a^{-1}{}_{ij})$ satisfies $AA^{-1} = I$ since $(AA^{-1})^j = A(A^{-1})^j = E^j$ is satisfied for each $j = 1, \ldots, n$.

Example 3.13 Let us find the inverse of the matrix A given by

$$\begin{pmatrix} -1 & 2 & 1 \\ 0 & 3 & -2 \\ 2 & -1 & 0 \end{pmatrix}$$

We leave it as an exercise for the reader to show that the reduced row-echelon form of

$$\begin{pmatrix} -1 & 2 & 1 & | & 1 & 0 & 0 \\ 0 & 3 & -2 & | & 0 & 1 & 0 \\ 2 & -1 & 0 & | & 0 & 0 & 1 \end{pmatrix}$$

is

$$\begin{pmatrix} 1 & 0 & 0 & | & 1/6 & 1/12 & 7/12 \\ 0 & 1 & 0 & | & 1/3 & 1/6 & 1/6 \\ 0 & 0 & 1 & | & 1/2 & -1/4 & 1/4 \end{pmatrix}$$

and hence A^{-1} is given by

$$\begin{pmatrix} 1/6 & 1/12 & 7/12 \\ 1/3 & 1/6 & 1/6 \\ 1/2 & -1/4 & 1/4 \end{pmatrix}. \;/\!\!/$$

Exercises

1. Verify the reduced row-echelon form of the matrix given in Example 3.13.

2. Find the inverse of a general 2 x 2 matrix. What constraints are there on the entries of the matrix?

3. Show that a matrix is not invertible if it has any zero row or column.

4. Find the inverse of each of the following matrices:

$$(a)\ \begin{pmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{pmatrix} \qquad (b)\ \begin{pmatrix} 1 & 3 & 4 \\ 3 & -1 & 6 \\ -1 & 5 & 1 \end{pmatrix} \qquad (c)\ \begin{pmatrix} 1 & 2 & 1 \\ 2 & 5 & 2 \\ 1 & 3 & 3 \end{pmatrix}$$

5. Use the inverse of the matrix in Exercise 4(c) above to find the solutions of each of the following systems:

$$(a)\ \begin{aligned} x + 2y + \ \ z &= 10 \\ 2x + 5y + 2z &= 14 \\ x + 3y + 3z &= 30 \end{aligned} \qquad (b)\ \begin{aligned} x + 2y + \ \ z &= \ \ 2 \\ 2x + 5y + 2z &= -1 \\ x + 3y + 3z &= \ \ 6 \end{aligned}$$

6. What is the inverse of a diagonal matrix?

7. (a) Prove that an upper-triangular matrix is invertible if and only if every entry on the main diagonal is nonzero (see Exercise 3.6.9 for the definition of an upper-triangular matrix).
(b) Prove that the inverse of a lower (upper) triangular matrix is lower (upper) triangular.

8. Find the inverse of the following matrix:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 3 & 4 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

9. (a) Let A be any 2 x 1 matrix, and let B be any 1 x 2 matrix. Prove that AB is not invertible.

(b) Repeat part (a) where A is any m x n matrix and B is any n x m matrix with $n < m$.

10. Summarize several of our results by proving the equivalence of the following statements for any n x n matrix A:
(a) A is invertible.
(b) The homogeneous system $AX = 0$ has only the zero solution.
(c) The system $AX = Y$ has a solution X for every n x 1 matrix Y.

11. Let A and B be square matrices of size n, and assume that A is nonsingular. Prove that $r(AB) = r(B) = r(BA)$.

12. A matrix A is called a **left zero divisor** if there exists a nonzero matrix B such that $AB = 0$, and A is called a **right zero divisor** if there exists a nonzero matrix C such that $CA = 0$. If A is an m x n matrix, prove that:
(a) If $m < n$, then A is a left zero divisor.
(b) If $m > n$, then A is a right zero divisor.
(c) If $m = n$, then A is both a left and a right zero divisor if and only if A is singular.

13. Let A and B be nonsingular symmetric matrices for which $AB - BA = 0$. Show that AB, $A^{-1}B$, AB^{-1} and $A^{-1}B^{-1}$ are all symmetric.

3.8 ELEMENTARY MATRICES

Recall the elementary row operations α, β, γ described in Section 3.2. We now let e denote any one of these three operations, and for any matrix A we define e(A) to be the result of applying the operation e to the matrix A. In particular, we define an **elementary matrix** to be any matrix of the form e(I). The great utility of elementary matrices arises from the following theorem.

Theorem 3.22 If A is any m x n matrix and e is any elementary row operation, then

$$e(A) = e(I_m)A\ .$$

Proof We must verify this equation for each of the three types of elementary row operations. First consider an operation of type α. In particular, let α be the interchange of rows i and j. Then

$$[e(A)]_k = A_k \quad \text{for } k \neq i, j$$

while

$$[e(A)]_i = A_j \quad \text{and} \quad [e(A)]_j = A_i \ .$$

On the other hand, using $(AB)_k = A_k B$ we also have

$$[e(I)A]_k = [e(I)]_k A \ .$$

If $k \neq i, j$ then $[e(I)]_k = I_k$ so that

$$[e(I)]_k A = I_k A = A_k \ .$$

If $k = i$, then $[e(I)]_i = I_j$ and

$$[e(I)]_i A = I_j A = A_j \ .$$

Similarly, we see that

$$[e(I)]_j A = I_i A = A_i \ .$$

This verifies the theorem for transformations of type α. (It may be helpful for the reader to write out e(I) and e(I)A to see exactly what is going on.)

There is essentially nothing to prove for type β transformations, so we go on to those of type γ. Hence, let e be the addition of c times row j to row i. Then

$$[e(I)]_k = I_k \quad \text{for } k \neq i$$

and

$$[e(I)]_i = I_i + cI_j \ .$$

Therefore

$$[e(I)]_i A = (I_i + cI_j)A = A_i + cA_j = [e(A)]_i$$

and for $k \neq i$ we have

$$[e(I)]_k A = I_k A = A_k = [e(A)]_k \ . \ \blacksquare$$

If e is of type α, then rows i and j are interchanged. But this is readily undone by interchanging the same rows again, and hence e^{-1} is defined and is another elementary row operation. For type β operations, some row is multiplied by a scalar c, so in this case e^{-1} is simply multiplication by 1/c. Finally, a type γ operation adds c times row j to row i, and hence e^{-1} adds $-c$ times row j to row i. Thus all three types of elementary row operations have inverses which are also elementary row operations.

By way of nomenclature, a square matrix $A = (a_{ij})$ is said to be **diagonal** if $a_{ij} = 0$ for $i \neq j$. The most common example of a diagonal matrix is the identity matrix.

Theorem 3.23 Every elementary matrix is nonsingular, and

$$[e(I)]^{-1} = e^{-1}(I) \ .$$

Furthermore, the transpose of an elementary matrix is an elementary matrix.

Proof By definition, e(I) is row equivalent to I and hence has the same rank as I (Theorem 3.4). Thus e(I) is nonsingular since $r(I_n) = n$, and hence $e(I)^{-1}$ exists. Since it was shown above that e^{-1} is an elementary row operation, we apply Theorem 3.22 to the matrix e(I) to obtain

$$e^{-1}(I)e(I) = e^{-1}(e(I)) = I \ .$$

Similarly, applying Theorem 3.22 to $e^{-1}(I)$ yields

$$e(I)e^{-1}(I) = e(e^{-1}(I)) = I \ .$$

This shows that $e^{-1}(I) = [e(I)]^{-1}$.

Now let e be a type α transformation that interchanges rows i and j (with $i < j$). Then the *ith* row of e(I) has a 1 in the *jth* column, and the *jth* row has a 1 in the *ith* column. In other words,

$$[e(I)]_{ij} = 1 = [e(I)]_{ji}$$

while for $r, s \neq i, j$ we have

$$[e(I)]_{rs} = 0 \quad \text{if } r \neq s$$

and

$$[e(I)]_{rr} = 1 \ .$$

Taking the transpose shows that

$$[e(I)]^T{}_{ij} = [e(I)]_{ji} = 1 = [e(I)]_{ij}$$

and

$$[e(I)]^T{}_{rs} = [e(I)]_{sr} = 0 = [e(I)]_{rs} \ .$$

Thus $[e(I)]^T = e(I)$ for type α operations.

Since I is a diagonal matrix, it is clear that for a type β operation which simply multiplies one row by a nonzero scalar, we have $[e(I)]^T = e(I)$.

Finally, let e be a type γ operation that adds c times row j to row i. Then e(I) is just I with the additional entry $[e(I)]_{ij} = c$, and hence $[e(I)]^T$ is just I with the additional entry $[e(I)]_{ji} = c$. But this is the same as c times row i added to row j in the matrix I. In other words, $[e(I)]^T$ is just another elementary matrix. ∎

We now come to the main result dealing with elementary matrices. For ease of notation, we denote an elementary matrix by E rather than by e(I). In other words, the result of applying the elementary row operation e_i to I will be denoted by the matrix $E_i = e_i(I)$.

Theorem 3.24 Every nonsingular n x n matrix may be written as a product of elementary n x n matrices.

Proof It follows from Theorem 3.10 that any nonsingular n x n matrix A is row equivalent to I_n. This means that I_n may be obtained by applying r successive elementary row operations to A. Hence applying Theorem 3.22 r times yields

$$E_r \cdots E_1 A = I_n$$

so that

$$A = E_1^{-1} \cdots E_r^{-1} I_n = E_1^{-1} \cdots E_r^{-1} \,.$$

The theorem now follows if we note that each E_i^{-1} is an elementary matrix according to Theorem 3.23 (since $E_i^{-1} = [e(I)]^{-1} = e^{-1}(I)$ and e^{-1} is an elementary row operation). ∎

Corollary If A is an invertible n x n matrix, and if some sequence of elementary row operations reduces A to the identity matrix, then the same sequence of row operations reduces the identity matrix to A^{-1}.

Proof By hypothesis we may write $E_r \cdots E_1A = I$. But then multiplying from the right by A^{-1} shows that $A^{-1} = E_r \cdots E_1I$. ∎

Note this corollary provides another proof that the method given in the previous section for finding A^{-1} is valid.

There is one final important property of elementary matrices that we will need in a later chapter. Let E be an n x n elementary matrix representing any of the three types of elementary row operations, and let A be an n x n matrix. As we have seen, multiplying A from the left by E results in a new matrix with the same rows that would result from applying the elementary row operation to A directly. We claim that multiplying A from the right by E^T results in a new matrix whose columns have the same relationship as the rows of EA. We will prove this for a type γ operation, leaving the easier type α and β operations to the reader (see Exercise 3.8.1).

Let γ be the addition of c times row j to row i. Then the rows of E are given by $E_k = I_k$ for $k \neq i$, and $E_i = I_i + cI_j$. Therefore the columns of E^T are given by

$$(E^T)^k = I^k \quad \text{for } k \neq i$$

and

$$(E^T)^i = I^i + cI^j\ .$$

Now recall that the k*th* column of AB is given by $(AB)^k = AB^k$. We then have

$$(AE^T)^k = A(E^T)^k = AI^k = A^k \quad \text{for } k \neq i$$

and

$$(AE^T)^i = A(E^T)^i = A(I^i + cI^j) = AI^i + cAI^j = A^i + cA^j\ .$$

This is the same relationship as that found between the rows of EA where $(EA)_k = A_k$ and $(EA)_i = A_i + cA_j$ (see the proof of Theorem 3.22).

Exercises

1. Let A be an n x n matrix, and let E be an n x n elementary matrix representing a type α or β operation. Show that the columns of AE^T have the same relationship as the rows of EA.

2. Write down 4 x 4 elementary matrices that will induce the following elementary operations in a 4 x 4 matrix when used as left multipliers. Verify that your answers are correct.
   (a) Interchange the 2*nd* and 4*th* rows of A.
   (b) Interchange the 2*nd* and 3*rd* rows of A.
   (c) Multiply the 4*th* row of A by 5.
   (d) Add k times the 4*th* row of A to the 1*st* row of A.
   (e) Add k times the 1*st* row of A to the 4*th* row of A.

3. Show that any $e_\alpha(A)$ may be written as a product of $e_\beta(A)$'s and $e_\gamma(A)$'s. (The notation should be obvious.)

4. Pick any 4 x 4 matrix A and multiply it from the *right* by each of the elementary matrices found in the previous problem. What is the effect on A?

5. Prove that a matrix A is row equivalent to a matrix B if and only if there exists a nonsingular matrix P such that B = PA.

6. Reduce the matrix

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & -1 \\ 2 & 3 & 3 \end{pmatrix}$$

to the reduced row-echelon form R, and write the elementary matrix corresponding to each of the elementary row operations required. Find a nonsingular matrix P such that PA = R by taking the product of these elementary matrices.

7. Let A be an n x n matrix. Summarize several of our results by proving that the following are equivalent:
(a) A is invertible.
(b) A is row equivalent to I_n .
(c) A is a product of elementary matrices.

8. Using the results of the previous problem, prove that if $A = A_1 A_2 \cdots A_k$ where each A_i is a square matrix, then A is invertible if and only if each of the A_i is invertible.

The remaining problems are all connected, and should be worked in the given order.

9. Suppose that we define elementary column operations exactly as we did for rows. Prove that every elementary column operation on A can be achieved by multiplying A on the *right* by an elementary matrix. [*Hint*: You can either do this directly as we did for rows, or by taking transposes and using Theorem 3.23.]

10. Show that an m x n reduced row-echelon matrix R of rank k can be reduced by elementary column operations to an m x n matrix C of the form

$$C = \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \end{pmatrix}$$

where the first k entries on the main diagonal are 1's, and the rest are 0's.

11. From the previous problem and Theorem 3.3, show that every m x n matrix A of rank k can be reduced by elementary row and column operations to the form C. We call the matrix C the **canonical form** of A.

12. We say that a matrix A is **row-column-equivalent** (abbreviated by r.c.e.) to a matrix B if A can be transformed into B by a finite number of elementary row and column operations. Prove:
(a) If A is a matrix, e is an elementary row operation, and e′ is an elementary column operation, then (eA)e′ = e(Ae′).
(b) r.c.e. is an equivalence relation.
(c) Two m x n matrices A and B are r.c.e. if and only if they have the same canonical form, and hence if and only if they have the same rank.

13. If A is any m x n matrix of rank k, prove that there exists a nonsingular m x m matrix P and a nonsingular n x n matrix Q such that PAQ = C (the canonical form of A).

14. Prove that two m x n matrices A and B are r.c.e. if and only if there exists a nonsingular m x m matrix P and a nonsingular n x n matrix Q such that PAQ = B.

CHAPTER 4

Determinants

Suppose we want to solve the system of equations

$$\begin{aligned} ax + by &= f \\ cx + dy &= g \end{aligned}$$

where a, b, c, d, f, g ∈ $\mathcal{F}$. It is easily verified that if we reduce the augmented matrix to reduced row-echelon form we obtain

$$\begin{pmatrix} 1 & 0 & (fd - gb)/\Delta \\ 0 & 1 & (ag - cf)/\Delta \end{pmatrix}$$

where Δ = ad − cb. We must therefore have Δ ≠ 0 if a solution is to exist for every choice of f and g. If A ∈ $M_2(\mathcal{F})$ is the matrix of coefficients of our system, we call the number Δ the **determinant** of A, and write this as det A. While it is possible to proceed from this point and define the determinant of larger matrices by induction, we prefer to take another more useful approach in developing the general theory. We will find that determinants arise in many different and important applications. Recall that unless otherwise noted, we always assume that $\mathcal{F}$ is not of characteristic 2 (see Exercise 1.5.15).

4.1 DEFINITIONS AND ELEMENTARY PROPERTIES

Recalling our discussion of permutations in Section 1.2 we make the following definition. If A = (a_{ij}) is an n x n matrix over a field $\mathcal{F}$, we define the **determinant** of A to be the scalar

$$\det A = \Sigma_{\sigma\in S_n}(\operatorname{sgn}\sigma)a_{1\sigma 1}a_{2\sigma 2}\cdots a_{n\sigma n}$$

where σi is the image of i = 1, . . . , n under the permutation σ. We frequently write the determinant as

$$\det A = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} \;.$$

Note that our definition contains n! terms in the sum, where each term is a product of n factors a_{ij} , and where each of these terms consists of precisely one factor from each row and each column of A. The determinant of an n x n matrix A is said to be of **order** n. We will sometimes denote the determinant of A by |A|. Note that the determinant is only defined for a square matrix.

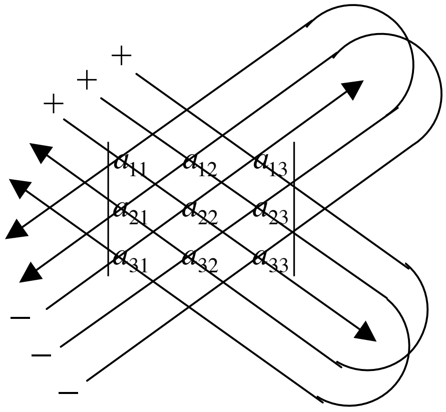
Example 4.1 We leave it to the reader to show that in the case of a 2 x 2 matrix, our definition agrees with the elementary formula

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - cb \;\;.$$

In the case of a 3 x 3 matrix, we have

$$\begin{aligned} \det A &= \Sigma_\sigma(\operatorname{sgn}\sigma)a_{1\sigma 1}a_{2\sigma 2}a_{3\sigma 3} \\ &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ &\qquad -a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} \;\;. \end{aligned}$$

The reader may recognize this from a more elementary course when written in the mnemonic form


+
+
+
a_{11} a_{12} a_{13}
a_{21} a_{22} a_{23}
a_{31} a_{32} a_{33}
–
–
–

Here, we are to add together all products of terms connected by a (+) line, and subtract all of the products connected by a (–) line. We will see in a later section that this 3 x 3 determinant may be expanded as a sum of three 2 x 2 determinants. ∕∕∕

Recall that a diagonal matrix A = (a_{ij}) is defined by the property that a_{ij} = 0 for i ≠ j. We therefore see that if A is any diagonal matrix, then

$$\det A = a_{11} \cdots a_{nn} = \prod_{i=1}^{n} a_{ii}$$

since only the identity permutation results in solely nonzero factors (see also Theorem 4.5 below). In particular, we have the simple but important result

$$\det I = 1 \;.$$

We now proceed to prove several useful properties of determinants.

Theorem 4.1 For any A ∈ $M_n(\mathcal{F})$ we have det A^T = det A.

Proof Consider one of the terms (sgn σ)$a_{1\,\sigma1} \cdots a_{n\,\sigma n}$ in det A. Then $a_{i\,\sigma i}$ is in the i*th* row and σi*th* column of A, and as i varies from 1 to n, so does σi. If we write any factor $a_{i\,\sigma i}$ as a_{ij}, then j = σi so that i = σ^{-1}j. By Theorem 1.5 we know that sgn σ^{-1} = sgn σ, and hence we can write our term as

$$(\operatorname{sgn} \sigma)\, a_{\sigma^{-1}1\,1} \cdots a_{\sigma^{-1}n\,n} = (\operatorname{sgn} \theta)\, a_{\theta1\,1} \cdots a_{\theta n\,n}$$

where θ = σ^{-1}. Therefore, since S_n = {θ = σ^{-1}: σ ∈ S_n}, we have

$$\begin{aligned}\det A &= \Sigma_{\sigma\in S_n} (\operatorname{sgn} \sigma) a_{1\;\sigma 1} \cdots a_{n\;\sigma n}\\ &= \Sigma_{\theta\in S_n} (\operatorname{sgn} \theta) a_{\theta 1\;1} \cdots a_{\theta n\;n} \;.\end{aligned}$$

But $a^T{}_{ij} = a_{ji}$ so that

$$\begin{aligned}\det A^T &= \Sigma_{\theta\in S_n}(\operatorname{sgn}\theta)a^T{}_{1\,\theta 1}\cdots a^T{}_{n\,\theta n}\\ &= \Sigma_{\theta\in S_n}(\operatorname{sgn}\theta)a_{\theta 1\,1}\cdots a_{\theta n\,n}\end{aligned}$$

and hence $\det A = \det A^T$. ∎

It will be very convenient for us to view the determinant of $A \in M_n(\mathcal{F})$ as a function of the row vectors A_i. When we wish to do this, we will write

$$\det A = \det(A_1, \dots, A_n) .$$

Now consider a matrix $A \in M_n(\mathcal{F})$ and assume that $A_1 = rB_1 + sC_1$ where $B_1 = (b_{11}, \dots, b_{1n})$ and $C_1 = (c_{11}, \dots, c_{1n})$ are any two arbitrary (row) vectors in $\mathcal{F}^n$, and $r, s \in \mathcal{F}$. We then have

$$\begin{aligned}\det A &= \det(A_1, \dots, A_n)\\ &= \det(rB_1 + sC_1, A_2, \dots, A_n)\\ &= \Sigma_{\sigma\in S_n}(\operatorname{sgn}\sigma)(rb_{1\,\sigma 1} + sc_{1\,\sigma 1})a_{2\,\sigma 2}\cdots a_{n\,\sigma n}\\ &= r\Sigma_{\sigma\in S_n}(\operatorname{sgn}\sigma)b_{1\,\sigma 1}a_{2\,\sigma 2}\cdots a_{n\,\sigma n}\\ &\qquad + s\Sigma_{\sigma\in S_n}(\operatorname{sgn}\sigma)c_{1\,\sigma 1}a_{2\,\sigma 2}\cdots a_{n\,\sigma n} .\end{aligned}$$

If we now let B be the matrix such that $B_i = A_i$ for $i = 2, \dots, n$ and C be the matrix such that $C_i = A_i$ for $i = 2, \dots, n$ we see that

$$\det A = r \det B + s \det C .$$

Generalizing slightly, we summarize this result as a theorem for easy reference.

Theorem 4.2 Let $A \in M_n(\mathcal{F})$ have row vectors $A_1, \dots, A_n$ and assume that for some $i = 1, \dots, n$ we have

$$A_i = rB_i + sC_i$$

where $B_i, C_i \in \mathcal{F}^n$ and $r, s \in \mathcal{F}$. Let $B \in M_n(\mathcal{F})$ have rows $A_1, \dots, A_{i-1}, B_i, A_{i+1}, \dots, A_n$ and $C \in M_n(\mathcal{F})$ have rows $A_1, \dots, A_{i-1}, C_i, A_{i+1}, \dots, A_n$. Then

$$\det A = r \det B + s \det C .$$

Corollary 1 Let $A \in M_n(\mathcal{F})$ have rows $A_1, \dots, A_n$ and suppose that for some $i = 1, \dots, n$ we have

$$A_i = \sum_{j=1}^{k} r_j B_j$$

where $B_j \in \mathcal{F}^n$ for $j = 1, \dots, k$ and each $r_j \in \mathcal{F}$. Then

$$\begin{aligned}\det A &= \det(A_1, \dots, A_{i-1}, \Sigma_{j=1}^{k} r_j B_j, A_{i+1}, \dots, A_n) \\ &= \sum_{j=1}^{k} r_j \det(A_1, \dots, A_{i-1}, B_j, A_{i+1}, \dots, A_n)\ .\end{aligned}$$

Proof This follows at once by induction from the theorem. ∎

Corollary 2 If any row of $A \in M_n(\mathcal{F})$ is zero, then $\det A = 0$.

Proof If any row of A is zero, then clearly one factor in each term of the sum $\det A = \Sigma_{\sigma\in S_n}(\operatorname{sgn}\sigma)a_{1\sigma 1} \cdots a_{n\sigma n}$ will be zero. (This also follows from Theorem 4.2 by letting $r = s = 0$.) ∎

Corollary 3 If $A \in M_n(\mathcal{F})$ and $r \in \mathcal{F}$, then $\det(rA) = r^n \det A$.

Proof Since $rA = (ra_{ij})$ we have

$$\begin{aligned}\det(rA) &= \Sigma_{\sigma\in S_n}(\operatorname{sgn}\sigma)(ra_{1\,\sigma 1})\cdots(ra_{n\,\sigma n}) \\ &= r^n \Sigma_{\sigma\in S_n}(\operatorname{sgn}\sigma)a_{1\,\sigma 1}\cdots a_{n\,\sigma n} \\ &= r^n \det A\ . \ \blacksquare\end{aligned}$$

For any $A \in M_n(\mathcal{F})$ and $\sigma \in S_n$, we let σA denote the matrix with rows $A_{\sigma 1}, \dots, A_{\sigma n}$. For example, if A and σ are given by

$$A = \begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{pmatrix} \qquad \text{and} \qquad \sigma = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

then

$$\sigma A = \begin{pmatrix}7 & 8 & 9\\ 1 & 2 & 3\\ 4 & 5 & 6\end{pmatrix}\ .$$

Theorem 4.3 For any $A \in M_n(\mathcal{F})$ and $\sigma \in S_n$ we have

$$\det(\sigma A) = (\operatorname{sgn}\sigma)\det A \ .$$

Proof First we note that by definition

$$\det(\sigma A) = \det(A_{\sigma 1}\ , \dots , A_{\sigma n}) = \textstyle\sum_{\phi \in S_n} (\operatorname{sgn}\phi)\, a_{\sigma 1\ \phi 1} \cdots a_{\sigma n\ \phi n} \ .$$

Now note that for each $i = 1, \dots , n$ there exists a $j \in \{1, \dots , n\}$ such that $\sigma j = i$. Then $j = \sigma^{-1} i$ and $\phi j = \phi\sigma^{-1} i = \theta i$ (where we have defined $\phi\sigma^{-1} = \theta$) so that

$$a_{\sigma j\ \phi j} = a_{i\ \theta i} \ .$$

Since σ is fixed we see that $S_n = \{\theta = \phi\sigma^{-1}\colon \phi \in S_n\}$, and since by Theorem 1.4 we have $\operatorname{sgn}\phi = \operatorname{sgn}(\theta\sigma) = (\operatorname{sgn}\theta)(\operatorname{sgn}\sigma)$, it follows that

$$\det(\sigma A) = \textstyle\sum_{\theta \in S_n} (\operatorname{sgn}\theta)(\operatorname{sgn}\sigma)\, a_{1\ \theta 1} \cdots a_{n\ \ \theta n} = (\operatorname{sgn}\sigma)\det A \ . \ ∎$$

Note that all we really did in this last proof was rearrange the terms of $\det(\sigma A)$ to where each product contained terms with the rows in natural (i.e., increasing) order. Since the sum is over all $\phi \in S_n$, this is then the same as summing over all $\theta \in S_n$ where $\theta = \phi\sigma^{-1}$.

Corollary 1 If $B \in M_n(\mathcal{F})$ is obtained from $A \in M_n(\mathcal{F})$ by interchanging two rows of A, then $\det B = -\det A$.

Proof If σ is a transposition, then $\operatorname{sgn}\sigma = -1$ so that $\det B = \det(\sigma A) = -\det A$. ∎

Corollary 2 If $A \in M_n(\mathcal{F})$ has two identical rows, then $\det A = 0$.

Proof If we let B be the matrix obtained by interchanging the two identical rows of A, then $\det A = \det B = -\det A$ implies that $\det A = 0$. ∎

Let us make two remarks. First, the reader should realize that because of Theorem 4.1, Theorems 4.2 and 4.3 along with their corollaries apply to columns as well as to rows. Our second rather technical remark is based on the material in Section 1.5. Note that our treatment of determinants has made no reference to the field of scalars with which we have been working. In particular, in proving Corollary 2 of Theorem 4.3, what we actually showed was that $\det A = -\det A$, and hence $2\det A = 0$. But if $\mathcal{F}$ happens to be of characteristic 2, then we can not conclude from this that $\det A = 0$. However, in this case it is possible to prove the corollary directly through use of the expansion by minors to be discussed in Section 4.3 (see Exercise 4.3.19). This is why we remarked earlier that we assume our fields are not of characteristic 2. In fact, for most applications, the reader could just as well assume that we are working over either the real or complex number fields exclusively.

4.2 ADDITIONAL PROPERTIES OF DETERMINANTS

In this section we present a number of basic properties of determinants that will be used frequently in much of our later work. In addition, we will prove that three fundamental properties possessed by any determinant are in fact sufficient to uniquely define any function that happens to have these same three properties (see Theorem 4.9 below).

Theorem 4.4 Suppose $A \in M_n(\mathcal{F})$ and let $B \in M_n(\mathcal{F})$ be row equivalent to A.

(a) If B results from the interchange of two rows of A, then det B = −det A.
(b) If B results from multiplying any row (or column) of A by a scalar k, then det B = k det A.
(c) If B results from adding a multiple of one row of A to another row, then det B = det A.

Proof By Corollary 1 of Theorem 4.3, a type α elementary row transformation merely changes the sign of det A. Next, Theorem 4.2 shows that a type β transformation multiplies det A by a nonzero scalar (choose r = constant and s = 0 in the statement of the theorem). Now consider a type γ transformation that adds k times row j to row i. Then $B_i = A_i + kA_j$ so that applying Theorem 4.2 and Corollary 2 of Theorem 4.3 we have

$$\begin{aligned}\det B &= \det(B_1, \dots, B_i, \dots, B_j, \dots, B_n)\\ &= \det(A_1, \dots, A_i + kA_j, \dots, A_j, \dots, A_n)\\ &= \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n)\\ &\qquad\qquad +k\det(A_1, \dots, A_j, \dots, A_j, \dots, A_n)\\ &= \det A + k\cdot 0\\ &= \det A\ .\ \blacksquare\end{aligned}$$

Corollary If R is the reduced row-echelon form of a matrix A, then det R = 0 if and only if det A = 0.

Proof This follows from Theorem 4.4 since A and R are row-equivalent. ∎

A matrix $A \in M_n(\mathcal{F})$ is said to be upper-triangular if $a_{ij} = 0$ for $i > j$. Similarly, A is said to be lower-triangular if $a_{ij} = 0$ for $i < j$. In other words, an upper-triangular matrix has all zeros below the main diagonal, and a lower-triangular matrix has all zeros above the main diagonal.

Theorem 4.5 If $A \in M_n(\mathcal{F})$ is a triangular matrix, then $\det A = \prod_{i=1}^n a_{ii}$.

Proof If A is lower-triangular, then A is of the form

$$\begin{pmatrix} a_{11} & 0 & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & 0 & \cdots & 0 \\ a_{31} & a_{32} & a_{33} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & a_{n4} & \cdots & a_{nn} \end{pmatrix} .$$

Since $\det A = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{1\,\sigma 1} \cdots a_{n\,\sigma n}$, we claim that the only nonzero term in the sum occurs when σ is equal to the identity permutation. To see this, consider the nonzero term $t = a_{1\,\sigma 1} \cdots a_{n\,\sigma n}$ for some $\sigma \in S_n$. Since $a_{ij} = 0$ for $i < j$, we must have $\sigma 1 = 1$ or else $a_{1\,\sigma 1} = 0 = t$. Now consider $a_{2\,\sigma 2}$. Since $\sigma 1 = 1$ we must have $\sigma 2 \neq 1$, and hence the fact that $a_{2\,\sigma 2} = 0$ for $2 < \sigma 2$ means that only the $\sigma 2 = 2$ term will be nonzero. Next, since $\sigma 1 = 1$ and $\sigma 2 = 2$, we must have $\sigma 3 \neq 1$ or 2 so that $a_{3\,\sigma 3} = 0$ for $3 < \sigma 3$ means that only $a_{3\,3}$ can contribute. Continuing in this manner, we see that only the term $t = a_{11} \cdots a_{nn}$ is nonzero, and hence

$$\det A = a_{11} \cdots a_{nn} = \prod_{i=1}^{n} a_{ii} \;.$$

If A is an upper-triangular matrix, then the theorem follows from Theorem 4.1. ∎

Corollary If $A = (a_{ij})$ is diagonal, then $\det A = \prod_i a_{ii}$.

It is an obvious corollary of this theorem that $\det I = 1$ as we mentioned before. Another extremely important result is the following.

Theorem 4.6 A matrix $A \in M_n(\mathcal{F})$ is singular if and only if $\det A = 0$.

Proof Let R be the reduced row-echelon form of A. If A is singular, then $r(A) < n$ so that by Theorem 3.9 there must be at least one zero row in the matrix R. Hence $\det R = 0$ by Theorem 4.2, Corollary 2, and therefore $\det A = 0$ by the corollary to Theorem 4.4.

Conversely, assume that $r(A) = n$. Then, by Theorem 3.10, we must have $R = I_n$ so that $\det R = 1$. Hence $\det A \neq 0$ by the corollary to Theorem 4.4. In other words, if $\det A = 0$ it follows that $r(A) < n$. ∎

We now prove that the determinant of a product of matrices is equal to the product of the determinants. Because of the importance of this result, we will present two different proofs. The first is based on the next theorem.

Theorem 4.7 If $E \in M_n(\mathcal{F})$ is an elementary matrix and $A \in M_n(\mathcal{F})$, then

$$\det(EA) = (\det E)(\det A) .$$

Proof Recall from Theorem 3.22 that $e(A) = e(I)A = EA$. First note that if e is of type α, then $\det E = -\det I = -1$ (Theorem 4.3, Corollary 1), and similarly $\det e(A) = -\det A$. Hence in this case we have

$$\det(EA) = \det e(A) = (-1)\det A = (\det E)(\det A) .$$

If e is of type β, then using Theorem 4.2 we have $\det E = \det e(I) = k \det I = k$ so that

$$\det(EA) = \det e(A) = k \det A = (\det E)(\det A) .$$

Finally, if e is of type γ, then Theorem 4.5 shows us that $\det E = \det e(I) = 1$ and hence

$$\begin{aligned}\det(EA) &= \det e(A)\\ &= \det A \quad \text{(see the proof of Theorem 4.4)}\\ &=(\det E)(\det A) .\end{aligned}$$

This proves the theorem for each of the three types of elementary row operations. ∎

Theorem 4.8 Suppose $A, B \in M_n(\mathcal{F})$. Then $\det(AB) = (\det A)(\det B)$.

Proof 1 If either A or B is singular, then so is AB (Corollary to Theorem 3.20). Hence (by Theorem 4.6) it follows that either $\det A = 0$ or $\det B = 0$, and also $\det(AB) = 0$. Therefore the theorem is true in this case.

Now assume that A and B are both nonsingular. From Theorem 3.24 we may write $A = E_1 \cdots E_r$ so that repeated application of Theorem 4.7 yields

$$\begin{aligned}\det AB &= \det(E_1\cdots E_r B)\\ &= \det E_1 \det(E_2\cdots E_r B)\\ &= \det E_1 \det E_2 \det(E_3\cdots E_r B)\\ &= \cdots = \det E_1 \cdots \det E_r \det B\\ &= \det E_1 \cdots \det E_{r-2} \det(E_{r-1} \det E_r) \det B\\ &= \cdots = \det(E_1\cdots E_r)\det B\\ &= (\det A)(\det B)\ .\ ∎\end{aligned}$$

Proof 2 If C = AB, then $C_i = (AB)_i = \sum_j a_{ij}B_j$ for each i = 1, . . . , n (see Section 3.6). From Corollary 1 of Theorem 4.2 we then have

$$\begin{aligned}\det C &= \det(C_1, \dots, C_n)\\ &= \det(\Sigma_{j_1} a_{1j_1} B_{j_1}, \dots, \Sigma_{j_n} a_{nj_n} B_{j_n})\\ &= \Sigma_{j_1} \cdots \Sigma_{j_n} a_{1j_1} \cdots a_{nj_n} \det(B_{j_1}, \dots, B_{j_n})\ .\end{aligned}$$

Now, according to Corollary 2 of Theorem 4.3 we must have $j_k \neq j_m$ (for k ≠ m) so that we need consider only those terms in this expression for det C in which $(j_1, \dots, j_n)$ is a permutation of (1, . . . , n). Therefore

$$\det C = \Sigma_{\sigma\in S_n} a_{1\ \sigma 1} \cdots a_{n\ \sigma n} \det(B_{\sigma 1}, \dots, B_{\sigma n})$$

and hence by Theorem 4.3 we have

$$\begin{aligned}\det C &= \Sigma_{\sigma\in S_n} a_{1\ \sigma 1} \cdots a_{n\ \sigma n} (\operatorname{sgn} \sigma) \det(B_1, \dots, B_n)\\ &= (\det B)\Sigma_{\sigma\in S_n} (\operatorname{sgn} \sigma) a_{1\ \sigma 1} \cdots a_{n\ \sigma n}\\ &= (\det B)(\det A)\ .\ ∎\end{aligned}$$

Corollary If $A \in M_n(\mathcal{F})$ is nonsingular, then $\det A^{-1} = (\det A)^{-1}$.

Proof If A is nonsingular, then A^{-1} exists by Theorem 3.21 so that $AA^{-1} = I$. Hence applying Theorem 4.8 shows that

$$1 = \det I = \det(AA^{-1}) = (\det A)(\det A^{-1})\ .$$

This implies

$$\det A^{-1} = (\det A)^{-1}\ .\ ∎$$

We now show that three of the properties possessed by any determinant are in fact sufficient to uniquely define the determinant as a function D:

$M_n(\mathcal{F}) \to \mathcal{F}$. By way of terminology, a function D: $M_n(\mathcal{F}) \to \mathcal{F}$ is said to be **multilinear** if it is linear in each of its components. In other words, if $D(A) = D(A_1, \ldots, A_n)$ and $A_i = B_i + C_i$ for any $i = 1, \ldots, n$ then

$$\begin{aligned} D(A) &= D(A_1, \ldots, A_{i-1}, B_i + C_i, A_{i+1}, \ldots, A_n) \\ &= D(A_1, \ldots, A_{i-1}, B_i, A_{i+1}, \ldots, A_n) \\ &\qquad\qquad + D(A_1, \ldots, A_{i-1}, C_i, A_{i+1}, \ldots, A_n) \end{aligned}$$

and if $A_i = kB_i$ for any $k \in \mathcal{F}$, then

$$D(A) = D(A_1, \ldots, kB_i, \ldots, A_n) = k\,D(A_1, \ldots, B_i, \ldots, A_n) \;.$$

Note Theorem 4.2 shows that our function det A is multilinear.

Next, we say that D: $M_n(\mathcal{F}) \to \mathcal{F}$ is **alternating** if $D(A) = 0$ whenever A has two identical rows. From Corollary 2 of Theorem 4.3 we see that det A is alternating. To see the reason for the word alternating, suppose that $A_i = A_j = B_i + C_i$ and D is both multilinear and alternating. Then

$$\begin{aligned} 0 = D(A) &= D(A_1, \ldots, A_i, \ldots, A_j, \ldots, A_n) \\ &= D(A_1, \ldots, B_i + C_i, \ldots, B_i + C_i, \ldots, A_n) \\ &= D(A_1, \ldots, B_i, \ldots, B_i + C_i, \ldots, A_n) \\ &\qquad\qquad + D(A_1, \ldots, C_i, \ldots, B_i + C_i, \ldots, A_n) \\ &= D(A_1, \ldots, B_i, \ldots, B_i, \ldots, A_n) \\ &\qquad\qquad + D(A_1, \ldots, B_i, \ldots, C_i, \ldots, A_n) \\ &\qquad\qquad + D(A_1, \ldots, C_i, \ldots, B_i, \ldots, A_n) \\ &\qquad\qquad + D(A_1, \ldots, C_i, \ldots, C_i, \ldots, A_n) \\ &= 0 + D(A_1, \ldots, B_i, \ldots, C_i, \ldots, A_n) \\ &\qquad\qquad + D(A_1, \ldots, C_i, \ldots, B_i, \ldots, A_n) + 0 \end{aligned}$$

so that

$$D(A_1, \ldots, B, \ldots, C, \ldots, A_n) = -D(A_1, \ldots, C, \ldots, B, \ldots, A_n) \;.$$

Thus, to say that D is alternating means that D(A) changes sign if two rows of A are interchanged.

Finally, let $\{E_i\}$ be the n row vectors of I_n (note that $E_1, \ldots, E_n$ form the standard basis for $\mathcal{F}^n$). Then, as we saw in Theorem 4.5,

$$\det(E_1, \ldots, E_n) = \det I = 1 \;.$$

If we consider a permutation $\sigma \in S_n$, then from Theorem 4.3 we see that

$$\det(E_{\sigma 1}, \dots, E_{\sigma n}) = (\operatorname{sgn}\sigma)\det(E_1, \dots, E_n) = \operatorname{sgn}\sigma \ .$$

We are now in a position to prove the uniqueness of the determinant function.

Theorem 4.9 Let D: $M_n(\mathcal{F}) \to \mathcal{F}$ be a multilinear and alternating function with the additional property that D(I) = 1. If $\tilde{D}$: $M_n(\mathcal{F}) \to \mathcal{F}$ is any other function with these properties, then $\tilde{D} = D$. In particular, the determinant is the only such function.

Proof It follows from the above discussion that our function det has all three of the properties given in the theorem, and hence we must show that it is the only such function. Let $A_1, \dots, A_n$ be any set of n vectors in $\mathcal{F}^n$, and define the function Δ: $\mathcal{F}^n \times \cdots \times \mathcal{F}^n \to \mathcal{F}$ by

$$\Delta(A_1, \dots, A_n) = D(A_1, \dots, A_n) - \tilde{D}(A_1, \dots, A_n) \ .$$

We must show that $\Delta(A_1, \dots, A_n) = 0$.

It should be clear that Δ is multilinear and alternating, but that

$$\Delta(I) = \Delta(E_1, \dots, E_n) = D(I) - \tilde{D}(I) = 0 \ .$$

Since $\{E_i\}$ is the standard basis $\mathcal{F}^n$, it follows that for any $A_i \in \mathcal{F}^n$ we have $A_i = \sum_j c_{ij} E_j$ for some set of scalars c_{ij}. Using this and the properties of Δ, we then have

$$\begin{aligned}\Delta(A_1, \dots, A_n) &= \Delta(\textstyle\sum_{j_1} c_{1j_1} E_{j_1}, \dots, \sum_{j_n} c_{nj_n} E_{j_n}) \\ &= \textstyle\sum_{j_1} \cdots \sum_{j_n} c_{1j_1} \cdots c_{nj_n} \Delta(E_{j_1}, \dots, E_{j_n}) \ .\end{aligned}$$

At this point, each j_k is summed from 1 to n. However, Δ is alternating so that $\Delta(E_{j_1}, \dots, E_{j_n}) = 0$ if $j_k = j_m$ for any k, m = 1, . . . , n. Therefore the nonzero terms occur only when $(j_1, \dots, j_n)$ is some permutation of $(1, \dots, n)$ and hence

$$\Delta(A_1, \dots, A_n) = \textstyle\sum_{\sigma \in S_n} c_{1\,\sigma 1} \cdots c_{n\,\sigma n} \Delta(E_{\sigma 1}, \dots, E_{\sigma n}) \ .$$

Since D and $\tilde{D}$ are alternating, we have

$$D(E_{\sigma 1}, \dots, E_{\sigma n}) = (\operatorname{sgn}\sigma)\, D(E_1, \dots, E_n) = (\operatorname{sgn}\sigma)\, D(I) = \operatorname{sgn}\sigma$$

and similarly for $\tilde{D}$ (note that this follows from Theorem 1.2). Therefore we find that

$$\begin{aligned}\Delta(E_{\sigma 1}, \dots, E_{\sigma n}) &= D(E_{\sigma 1}, \dots, E_{\sigma n}) - \tilde{D}(E_{\sigma 1}, \dots, E_{\sigma n}) \\ &= \operatorname{sgn} \sigma - \operatorname{sgn} \sigma = 0\end{aligned}$$

and hence $\Delta(A_1, \dots, A_n) = 0$. ∎

Suppose that D is a multilinear and alternating function on the set of all n-square matrices over $\mathcal{F}$. (Here we do not require that D(I) = 1.) If we write the rows of a matrix $A \in M_n(\mathcal{F})$ as $A_1, \dots, A_n$ then

$$A_i = \sum_{j=1}^{n} a_{ij} E_j$$

where $\{E_j\}$ are the rows of the identity matrix I_n. Exactly as we did in the preceding proof for the function Δ, we may write

$$\begin{aligned}D(A) &= D(A_1, \dots, A_n) \\ &= D(\Sigma_{j_1} a_{1j_1} E_{j_1}, \dots, \Sigma_{j_n} a_{nj_n} E_{j_n}) \\ &= \Sigma_{j_1 \cdots j_n} a_{1j_1} \cdots a_{nj_n} D(E_{j_1}, \dots, E_{j_n}) \\ &= \Sigma_{\sigma \in S_n} a_{1\,\sigma 1} \cdots a_{n\,\sigma n} D(E_{\sigma 1}, \dots, E_{\sigma n}) \\ &= \Sigma_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{1\,\sigma 1} \cdots a_{n\,\sigma n} D(E_1, \dots, E_n) \\ &= (\det A)\, D(I)\ .\end{aligned}$$

Note that this is actually a quite general formula, and says that any multilinear and alternating function D defined on $A \in M_n(\mathcal{F})$ is just the determinant of A times D(I). We will use this formula later in the chapter to give a simple proof of the formula for the determinant of a block triangular matrix.

Exercises

1. Compute the determinants of the following matrices directly from the definition:

$$(a)\ \begin{pmatrix} 1 & 2 & 3 \\ 4 & -2 & 3 \\ 2 & 5 & -1 \end{pmatrix} \qquad (b)\ \begin{pmatrix} 2 & 0 & 1 \\ 3 & 2 & -3 \\ -1 & -3 & 5 \end{pmatrix}$$

2. Consider the following real matrix:

$$A = \begin{pmatrix} 2 & 1 & 9 & 1 \\ 4 & 3 & -1 & 2 \\ 1 & 4 & 3 & 2 \\ 3 & 2 & 1 & 4 \end{pmatrix} .$$

Evaluate det A by reducing A to upper-triangular form and using Theorem 4.4.

3. Using the definition, show that

$$\begin{vmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{vmatrix} = a_1 \begin{vmatrix} b_2 & b_3 & b_4 \\ c_2 & c_3 & c_4 \\ d_2 & d_3 & d_4 \end{vmatrix} .$$

4. Evaluate the determinant of the following matrix:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix} .$$

5. If A is nonsingular and $A^{-1} = A^T$, show that det A = ±1 (such a matrix A is said to be **orthogonal**).

6. Consider a complex matrix $U \in M_n(\mathbb{C})$.
(a) If $U^* = (u_{ij}{}^*)$, show that det U^* = (det U)*.
(b) Let $U^\dagger = U^{*T}$ (this is called the **adjoint** or **conjugate transpose** of U, and is not to be confused with the classical adjoint introduced in the next section). Suppose U is such that $U^\dagger U = UU^\dagger = I$ (such a U is said to be **unitary**). Show that we may write $\det U = e^{i\phi}$ for some real ϕ.

7. If A is an n x n matrix and k is a scalar, show that:
(a) $\det(kA) = k^n \det A$ using Theorem 4.4(b).
(b) $\det A^n = (\det A)^n$.

8. (a) If A is a real n x n matrix and k is a positive odd integer, show that $A^k = I_n$ implies that det A = 1.

   (b) If $A^n = 0$ for some positive integer n, show that det A = 0. (A matrix for which $A^n = 0$ is said to be **nilpotent**.)

9. If the **anticommutator** $[A, B]_+ = AB + BA = 0$, show that A and/or B in $M_n(\mathcal{F})$ must be singular if n is odd. What can you say if n is even?

10. Suppose C is a 3 x 3 matrix that can be expressed as the product of a 3 x 2 matrix A and a 2 x 3 matrix B. Show that det C = 0. Generalize this result to n x n matrices.

11. Recall that A is **symmetric** if $A^T = A$. If A is symmetric, show that

$$\det(A + B) = \det(A + B^T) \ .$$

12. Recall that a matrix $A = (a_{ij})$ is said to be **antisymmetric** if $A^T = -A$, i.e., $a^T{}_{ij} = -a_{ji}$. If A is an antisymmetric square matrix of odd size, prove that det A = 0.

13. (a) Recall (see Exercise 3.6.7) that if $A \in M_n(\mathcal{F})$, then $\mathrm{Tr}\, A = \sum_i a_{ii}$. If A is a 2 x 2 matrix, prove that det(I + A) = 1 + det A if and only if Tr A = 0. Is this true for any size square matrix?

    (b) If $|a_{ij}| \ll 1$, show $\det(I + A) \cong 1 + \mathrm{Tr}\, A$.

14. Two matrices A and A′ are said to be **similar** if there exists a nonsingular matrix P such that $A' = PAP^{-1}$. The operation of transforming A into A′ in this manner is called a **similarity transformation**.

    (a) Show that this defines an equivalence relation on the set of all matrices.

    (b) Show that the determinant is invariant under a similarity transformation.

    (c) Show that the trace (Exercise 3.6.7) is also invariant.

15. Consider the matrices

$$A = \begin{pmatrix} 2 & 0 & -1 \\ 3 & 0 & 2 \\ 4 & -3 & 7 \end{pmatrix} \qquad B = \begin{pmatrix} 3 & 2 & -4 \\ 1 & 0 & -2 \\ -2 & 3 & 3 \end{pmatrix}$$

    (a) Evaluate det A and det B.

(b) Find AB and BA.
(c) Evaluate det AB and det BA.

16. Show that

$$\begin{vmatrix} a_1 & b_1 + xa_1 & c_1 + yb_1 + za_1 \\ a_2 & b_2 + xa_2 & c_2 + yb_2 + za_2 \\ a_3 & b_3 + xa_3 & c_3 + yb_3 + za_3 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} .$$

17. Find all values of x for which each of the following determinants is zero:

$$(a) \begin{vmatrix} x-1 & 1 & 1 \\ 0 & x-4 & 1 \\ 0 & 0 & x-2 \end{vmatrix} \qquad (b) \begin{vmatrix} 1 & x & x \\ x & 1 & x \\ x & x & 1 \end{vmatrix}$$

$$(c) \begin{vmatrix} 1 & x & x^2 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{vmatrix}$$

18. Show that
(a) $\det(A_1 + A_2, A_2 + A_3, A_3 + A_1) = 2 \det(A_1, A_2, A_3)$.
(b) $\det(A_1 + A_2, A_2 + A_3, A_3 + A_4, A_4 + A_1) = 0$.

19. Given a matrix A, the matrix that remains after any rows and/or columns of A have been deleted is called a **submatrix** of A, and the determinant of a square submatrix is called a **subdeterminant**. Show that the rank of a matrix A is the size of the largest nonvanishing subdeterminant of A. [*Hint*: Think about Theorem 3.9, Corollary 2 of Theorem 4.2, and Theorem 4.4.]

20. Show that the following determinant is zero:

$$\begin{vmatrix} a^2 & (a+1)^2 & (a+2)^2 & (a+3)^2 \\ b^2 & (b+1)^2 & (b+2)^2 & (b+3)^2 \\ c^2 & (c+1)^2 & (c+2)^2 & (c+3)^2 \\ d^2 & (d+1)^2 & (d+2)^2 & (d+3)^2 \end{vmatrix}$$

[*Hint*: You need not actually evaluate it.]

21. Show that

$$\begin{vmatrix} 1 & 6 & 11 & 16 & 21 \\ 2 & 7 & 12 & 17 & 22 \\ 3 & 8 & 13 & 18 & 23 \\ 4 & 9 & 14 & 19 & 24 \\ 5 & 10 & 15 & 20 & 25 \end{vmatrix} = 0 \;.$$

22. (a) If E is an elementary matrix, show (without using Theorem 4.1) that det E^T = det E.

    (b) Use Theorem 3.24 to show that det A^T = det A for any $A \in M_n(\mathcal{F})$.

23. Use the material of this section to give a proof (independent of Chapter 3) that the product of nonsingular matrices is nonsingular.

4.3 EXPANSION BY MINORS

We now turn our attention to methods of evaluating determinants. Since S_n contains n! elements, it is obvious that using our definition of det A becomes quite impractical for any n much larger than four. Before proceeding with the general theory of minors, let us first present a method of evaluating determinants that is based on Theorem 4.5. All we have to do is reduce the matrix to triangular form, being careful to keep track of each elementary row operation along the way, and use Theorem 4.4. One example should suffice to illustrate the procedure.

Example 4.2 Consider the matrix A given by

$$A = \begin{pmatrix} 2 & -1 & 3 \\ 1 & 2 & -1 \\ -3 & 0 & 2 \end{pmatrix} \;.$$

Then we have

$$\det A = \begin{vmatrix} 2 & -1 & 3 \\ 1 & 2 & -1 \\ -3 & 0 & 2 \end{vmatrix}$$

$$= 2\begin{vmatrix} 1 & -1/2 & 3/2 \\ 1 & 2 & -1 \\ -3 & 0 & 2 \end{vmatrix} \begin{matrix} \leftarrow (1/2)A_1 \\ \\ \\ \end{matrix}$$

$$= 2\begin{vmatrix} 1 & -1/2 & 3/2 \\ 0 & 5/2 & -5/2 \\ 0 & -3/2 & 13/2 \end{vmatrix} \begin{matrix} \\ \leftarrow -A_1 + A_2 \\ \leftarrow 3A_1 + A_3 \end{matrix}$$

$$= 2\begin{vmatrix} 1 & -1/2 & 3/2 \\ 0 & 5/2 & -5/2 \\ 0 & 0 & 5 \end{vmatrix} \begin{matrix} \\ \\ \leftarrow (3/5)A_2 + A_3 \end{matrix}$$

$$= (2)(1)(5/2)(5) = 25 .$$

The reader should verify this result by the direct calculation of det A. ∫∫

We now begin our discussion of the expansion by minors. Suppose A = $(a_{ij}) \in M_n(\mathcal{F})$, and note that for any term $a_{r\,\sigma r}$ in the definition of det A and for any s = 1, . . . , n we may factor out all terms with σr = s and then sum over all s. This allows us to write

$$\begin{aligned} \det A &= \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma) a_{1\,\sigma1} \cdots a_{r\,\sigma r} \cdots a_{n\,\sigma n} \\ &= \sum_{s=1}^{n} a_{rs} \sum_{\sigma\in S_n,\ \sigma r = s} (\operatorname{sgn}\sigma) a_{1\,\sigma1} \cdots a_{r-1\,\sigma(r-1)} a_{r+1\,\sigma(r+1)} \cdots a_{n\,\sigma n} \\ &= \sum_{s=1}^{n} a_{rs} a'_{rs} \end{aligned}$$

where $\sum_{\sigma\in S_n,\ \sigma r = s}$ means to sum over all σ ∈ S_n subject to the condition that σr = s, and

$$a'_{rs} = \sum_{\sigma\in S_n,\ \sigma r = s} (\operatorname{sgn}\sigma) a_{1\,\sigma1} \cdots a_{r-1\,\sigma(r-1)} a_{r+1\,\sigma(r+1)} \cdots a_{n\,\sigma n} \quad .$$

The term a'_{rs} is called the **cofactor** of a_{rs} . Since the sum is over all σ ∈ S_n subject to the condition σr = s, we see that a'_{rs} contains (n - 1)! terms. Indeed, it should be apparent that a'_{rs} looks very much like the determinant of some (n - 1) x (n - 1) matrix.

To see that this is in fact the case, we define the matrix $A_{rs} \in M_{n-1}(\mathcal{F})$ to be the matrix obtained from A ∈ $M_n(\mathcal{F})$ by deleting the r*th* row and s*th* column of A. The matrix A_{rs} is called the rs*th* **minor matrix** of A, and det A_{rs} is called the rs*th* **minor** of A. We now prove the method of calculating det A known as the "expansion by minors."

Theorem 4.10 Suppose $A = (a_{ij}) \in M_n(\mathcal{F})$. Then for any r = 1, . . . , n we have

$$\det A = \sum_{s=1}^{n} a_{rs}a'_{rs}$$

where

$$a'_{rs} = (-1)^{r+s}\det A_{rs} \quad .$$

Proof We saw above that $\det A = \sum_{s=1}^{n} a_{rs}a'_{rs}$ where each a'_{rs} depends only on those elements of A that are not in the r*th* row or the s*th* column. In particular, consider the expansion $\det A = a_{11}a'_{11} + \cdots + a_{1n}a'_{1n}$ and look at the coefficient a'_{11} of a_{11}. By definition, we have

$$a'_{11} = \sum_{\sigma\in S_n,\ \sigma 1=1} (\operatorname{sgn}\sigma)a_{2\ \sigma 2}\cdots a_{n\ \sigma n}$$

where each term in the sum is a product of elements, one from each row and one from each column of A except for the first row and column, and the sum is over all possible permutations of the remaining n - 1 columns. But this is precisely the definition of det A_{11}, and hence $a'_{11} = \det A_{11}$. (Remember that the r*th* row of A_{11} is $(A_{11})_r = (a_{r+1\ 2}, \dots, a_{r+1\ n})$.)

We now need to find the coefficient a'_{rs} for any a_{rs}. To do this, we start with the matrix A, and then move the r*th* row up to be the new first row, and move the s*th* column left to be the new first column. This defines a new matrix B such that $b_{11} = a_{rs}$ and $B_{11} = A_{rs}$ (note this implies that $\det B_{11} = \det A_{rs}$). Moving the r*th* row involves r - 1 interchanges, and moving the s*th* column involves s - 1 interchanges. Hence applying Corollary 1 of Theorem 4.3 to both rows and columns, we see that

$$\det B = (-1)^{r+s-2}\det A = (-1)^{r+s}\det A \ .$$

If we expand det B by the first row and expand det A by the r*th* row, we find

$$\sum_{p=1}^{n} b_{1p}b'_{1p} = \det B = (-1)^{r+s}\det A = (-1)^{r+s}\sum_{p=1}^{n} a_{rp}a'_{rp} \quad .$$

Now remember that the set $\{b_{11}, \dots, b_{1n}\}$ is just the set $\{a_{r1}, \dots, a_{rn}\}$ taken in a different order where, in particular, $b_{11} = a_{rs}$. Since the r*th* row of A is arbitrary, we may assume that $a_{rj} = 0$ for all $j \neq s$. In this case, we have

$$\det B = b_{11}b'_{11} = (-1)^{r+s}\det A = (-1)^{r+s} a_{rs}\, a'_{rs}$$

where $b_{11} = a_{rs}$, and therefore

$$b'_{11} = (-1)^{r+s} a'_{rs}$$

or

$$a'_{rs} = (-1)^{r+s} b'_{11} \; .$$

At the beginning of this proof we showed that $a'_{11} = \det A_{11}$, and hence an identical argument shows that $b'_{11} = \det B_{11}$. Putting all of this together then results in

$$a'_{rs} = (-1)^{r+s} b'_{11} = (-1)^{r+s} \det B_{11} = (-1)^{r+s} \det A_{rs} \; . \;\blacksquare$$

The reader may find it helpful to repeat this proof by moving the r*th* row down and the s*th* column to the right so that $b_{nn} = a_{rs}$. In this case, instead of a_{11} we consider

$$a'_{nn} = \sum_{\sigma \in S_n,\; \sigma n = n} (\operatorname{sgn} \sigma) a_{1\,\sigma 1} \cdots a_{n-1\;\sigma(n-1)}$$

which is just $\det A_{nn}$ since $A_{nn} \in M_{n-1}(\mathcal{F})$ and the sum over all $\sigma \in S_n$ subject to $\sigma n = n$ is just the sum over all $\sigma \in S_{n-1}$. It then follows again that $b'_{nn} = \det B_{nn} = \det A_{rs}$ and $b'_{nn} = (-1)^{r+s} a'_{rs}$.

Corollary 1 Using the same notation as in Theorem 4.10, for any s = 1, . . . , n we have

$$\det A = \sum_{r=1}^{n} a_{rs} a'_{rs} \quad .$$

(Note that here det A is expanded by the s*th* column, whereas in Theorem 4.10 det A was expanded by the r*th* row.)

Proof This follows by applying Theorem 4.10 to A^T and then using Theorem 4.1. ∎

Theorem 4.10 is called **expansion by minors** of the r*th* row, and Corollary 1 is called **expansion by minors** of the s*th* column. (See also Exercise 11.3.9.)

Corollary 2 Using the same notation as in Theorem 4.10, we have

$$\sum_{s=1}^{n} a_{ks}a'_{ks} = 0 \qquad \text{if } k \neq r$$

$$\sum_{r=1}^{n} a_{rk}a'_{rk} = 0 \qquad \text{if } k \neq s \ \ .$$

Proof Given A = $(a_{ij}) \in M_n(\mathcal{F})$, we define B $\in M_n(\mathcal{F})$ by $B_i = A_i$ for i ≠ r and $B_r = A_k$ where r ≠ k. In other words, we replace the r*th* row of A by the k*th* row of A to obtain B. Since B has two identical rows, it follows that det B = 0. Noting that $B_{rs} = A_{rs}$ (since both minor matrices delete the r*th* row), we see that $b'_{rs} = a'_{rs}$ for each s = 1, . . . , n. We therefore have

$$0 = \det B = \sum_{s=1}^{n} b_{rs}b'_{rs} = \sum_{s=1}^{n} b_{rs}a'_{rs} = \sum_{s=1}^{n} a_{ks}a'_{rs} \ \ .$$

Similarly, the other result follows by replacing the s*th* column of A by the k*th* column so that $b_{rs} = a_{rk}$, and then using Corollary 1. ∎

Example 4.3 Consider the matrix A given by

$$A = \begin{pmatrix} 2 & -1 & 5 \\ 0 & 3 & 4 \\ 1 & 2 & -3 \end{pmatrix} \ .$$

To illustrate the terminology, note that the (2, 3) minor matrix is given by

$$A_{23} = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$$

and hence the (2, 3) minor of A is det $A_{23} = 4 - (-1) = 5$, while the (2, 3) cofactor of A is $(-1)^{2+3} \det A_{23} = -5$.

We now wish to evaluate det A. Expanding by the second row we have

$$\begin{aligned} \det A &= a_{21}a'_{21} + a_{22}a'_{22} + a_{23}a'_{23} \\ &= 0 + (-1)^4(3)\begin{vmatrix} 2 & 5 \\ 1 & -3 \end{vmatrix} + (-1)^5(4)\begin{vmatrix} 2 & -1 \\ 1 & 2 \end{vmatrix} \\ &= 3(-6-5) - 4(4+1) = -53 \ \ . \end{aligned}$$

The reader should repeat this using other rows and columns to see that they all yield the same result. ∕∕

Example 4.4 Let us evaluate det A where A is given by

$$A=\begin{pmatrix} 5 & 4 & 2 & 1\\ 2 & 3 & 1 & -2\\ -5 & -7 & -3 & 9\\ 1 & -2 & -1 & 4\end{pmatrix}\,.$$

In view of Theorem 4.4, we first perform the following elementary row operations on A: (*i*) $A_1 \to A_1 - 2A_2$, (*ii*) $A_3 \to A_3 + 3A_2$, (*iii*) $A_4 \to A_4 + A_2$. This results in the following matrix B:

$$B=\begin{pmatrix} 1 & -2 & 0 & 5\\ 2 & 3 & 1 & -2\\ 1 & 2 & 0 & 3\\ 3 & 1 & 0 & 2\end{pmatrix}\,.$$

Since these were all type γ operations it follows that det B = det A, and hence expanding by minors of the third column yields only the single term

$$\det A=(-1)^{2+3}\begin{vmatrix} 1 & -2 & 5\\ 1 & 2 & 3\\ 3 & 1 & 2\end{vmatrix}\,.$$

This is easily evaluated either directly or by reducing to a sum of three 2 x 2 determinants. In any case, the result is det A = 38. ∕∕

We are now in a position to prove a general formula for the inverse of a matrix. Combining Theorem 4.10 and its corollaries, we obtain (for k, r, s = 1, . . . , n)

$$\sum_{s=1}^{n} a_{ks}a'_{rs}=\delta_{kr}\det A \tag{1a}$$

$$\sum_{r=1}^{n} a_{rk}a'_{rs}=\delta_{ks}\det A \tag{1b}$$

Since each $a'_{ij} \in \mathcal{F}$, we may use the them to form a new matrix $(a'_{ij}) \in M_n(\mathcal{F})$. The transpose of this new matrix is called the **adjoint** of A (or sometimes the **classical adjoint** to distinguish it from another type of adjoint to be discussed later) and is denoted by adj A. In other words,

$$\text{adj } A = (a'_{ij})^T\,.$$

Noting that $I_{ij} = \delta_{ij}$, it is now easy to prove the following.

Theorem 4.11 For any $A \in M_n(\mathcal{F})$ we have A(adj A) = (det A)I = (adj A)A. In particular, if A is nonsingular, then

$$A^{-1} = \frac{\operatorname{adj} A}{\det A}\;\;.$$

Proof Using $(\operatorname{adj} A)_{sr} = a'_{rs}$, we may write equation (1a) in matrix form as

$$A(\operatorname{adj} A) \;=\; (\det A)I$$

and equation (1b) as

$$(\operatorname{adj} A)A \;=\; (\det A)I\;\;.$$

Therefore, if A is nonsingular then det A ≠ 0 (Theorem 4.6), and hence

$$A(\operatorname{adj} A)/\det A \;=\; I \;=\; (\operatorname{adj} A)A/\det A\;\;.$$

Thus the uniqueness of the inverse (Theorem 3.21, Corollary 1) implies that

$$A^{-1} \;=\; (\operatorname{adj} A)/\det A\;\;. \;\blacksquare$$

It is important to realize that the equations

$$A(\operatorname{adj} A) \;=\; (\det A)I$$

and

$$(\operatorname{adj} A)A \;=\; (\det A)I$$

are valid even if A is singular. We will use this fact in Chapter 8 when we present a very simple proof of the Cayley-Hamilton Theorem.

Example 4.5 Let us use this method to find the inverse of the matrix

$$A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 3 & -2 \\ 2 & -1 & 0 \end{pmatrix}$$

used in Example 3.11. Leaving the details to the reader, we evaluate the cofactors using the formula $a'_{rs} = (-1)^{r+s} \det A_{rs}$ to obtain $a'_{11} = -2$, $a'_{12} = -4$,

$a'_{13} = -6$, $a'_{21} = -1$, $a'_{22} = -2$, $a'_{23} = 3$, $a'_{31} = -7$, $a'_{32} = -2$, and $a'_{33} = -3$. Hence we find

$$\operatorname{adj} A = \begin{pmatrix} -2 & -1 & -7 \\ -4 & -2 & -2 \\ -6 & 3 & -3 \end{pmatrix}.$$

To evaluate det A, we may either calculate directly or by minors to obtain det A = −12. Alternatively, from equation (1a) we have

$$\begin{aligned}(\det A)I = A(\operatorname{adj} A) &= \begin{pmatrix} -1 & 2 & 1 \\ 0 & 3 & -2 \\ 2 & -1 & 0 \end{pmatrix}\begin{pmatrix} -2 & -1 & -7 \\ -4 & -2 & -2 \\ -6 & 3 & -3 \end{pmatrix} \\ &= \begin{pmatrix} -12 & 0 & 0 \\ 0 & -12 & 0 \\ 0 & 0 & -12 \end{pmatrix} = -12\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\end{aligned}$$

so that we again find that det A = −12. In any case, we see that

$$A^{-1} = \frac{\operatorname{adj} A}{-12} = \begin{pmatrix} 1/6 & 1/12 & 7/12 \\ 1/3 & 1/6 & 1/6 \\ 1/2 & -1/4 & 1/4 \end{pmatrix}$$

which agrees with Example 3.11 as it should. ∞

If the reader thinks about Theorem 3.9, Corollary 2 of Theorem 4.2, and Theorem 4.4 (or has already worked Exercise 4.2.19), our next theorem should come as no real surprise. By way of more terminology, given a matrix A, the matrix that remains after any rows and/or columns have been deleted is called a **submatrix** of A. (A more precise definition is given in Section 4.6.)

Theorem 4.12 Let A be a matrix in $M_{m\mathrm{x}n}(\mathcal{F})$, and let k be the largest integer such that some submatrix $B \in M_k(\mathcal{F})$ of A has a nonzero determinant. Then r(A) = k.

Proof Since B is a k x k submatrix of A with det B ≠ 0, it follows from Theorem 4.6 that B is nonsingular and hence r(B) = k. This means that the k rows of B are linearly independent, and hence the k rows of A that contain the rows of B must also be linearly independent. Therefore r(A) = rr(A) ≥ k. By definition of k, there can be no r x r submatrix of A with nonzero determinant if r > k. We will now show that if r(A) = r, then there necessarily exists an r x r submatrix with nonzero determinant. This will prove that r(A) = k.

If r(A) = r, let A′ be the matrix with r linearly independent rows A_{i_1} , . . . , A_{i_r}. Clearly r(A′) = r also. But by definition of rank, we can also choose r linearly independent columns of A′. This results in a nonsingular matrix A″ of size r, and hence det A″ ≠ 0 by Theorem 4.6. ∎

Exercises

1. Verify the result of Example 4.2 by direct calculation.

2. Verify the result of Example 4.4.

3. Verify the terms a'_{ij} in Example 4.5.

4. Evaluate the following determinants by expanding by minors of either rows or columns:

$$(a)\ \begin{vmatrix} 2 & -1 & 5 \\ 0 & 3 & 4 \\ 1 & 2 & -3 \end{vmatrix} \qquad (b)\ \begin{vmatrix} 2 & 5 & 5 & 3 \\ 7 & -8 & 2 & 3 \\ 1 & -1 & 4 & -2 \\ -3 & 9 & -1 & 3 \end{vmatrix}$$

$$(c)\ \begin{vmatrix} 3 & 2 & 2 & 3 \\ 1 & -4 & 2 & 1 \\ 4 & 5 & -1 & 0 \\ -1 & -4 & 2 & 7 \end{vmatrix} \qquad (d)\ \begin{vmatrix} 3 & 1 & 0 & 4 & 2 & 1 \\ 2 & 0 & 1 & 0 & 5 & 1 \\ 0 & 4 & -1 & 1 & -1 & 2 \\ 0 & 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{vmatrix}$$

5. Let A ∈ $M_n(\mathcal{F})$ be a matrix with 0's down the main diagonal and 1's elsewhere. Show that det A = n − 1 if n is odd, and det A = 1 − n if n is even.

6. (a) Show that the determinant of the matrix

$$\begin{pmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{pmatrix}$$

is (c − a)(c − b)(b − a).

(b) Consider the matrix $V_n \in M_n(\mathcal{F})$ defined by

$$\begin{pmatrix} 1 & x_1 & {x_1}^2 & \cdots & {x_1}^{n-1} \\ 1 & x_2 & {x_2}^2 & \cdots & {x_2}^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & {x_n}^2 & \cdots & {x_n}^{n-1} \end{pmatrix} .$$

Prove that

$$\det V_n = \prod_{i<j} (x_j - x_i)$$

where the product is over all pairs i and j satisfying $1 \le i, j \le n$. This matrix is called the **Vandermonde matrix** of order n. [*Hint*: This should be done by induction on n. The idea is to show that

$$\det V_n = (x_2 - x_1)(x_3 - x_1) \cdots (x_{n-1} - x_1)(x_n - x_1) \det V_{n-1} .$$

Perform elementary column operations on V_n to obtain a new matrix V'_n with a 1 in the (1, 1) position and 0's in every other position of the first row. Now factor out the appropriate term from each of the other rows.]

7. The obvious method for deciding if two quadratic polynomials have a common root involves the quadratic formula, and hence taking square roots. This exercise investigates an alternative "root free" approach. (While we will define roots of polynomials in a later chapter, we assume that the reader knows that x_0 is a root of the polynomial p(x) if and only if $p(x_0) = 0$.)

(a) Show that

$$\det A = \begin{vmatrix} 1 & -(x_1 + x_2) & x_1 x_2 & 0 \\ 0 & 1 & -(x_1 + x_2) & x_1 x_2 \\ 1 & -(y_1 + y_2) & y_1 y_2 & 0 \\ 0 & 1 & -(y_1 + y_2) & y_1 y_2 \end{vmatrix}$$

$$= (x_1 - y_1)(x_1 - y_2)(x_2 - y_1)(x_2 - y_2) .$$

(b) Using this result, show that the polynomials

$$\begin{aligned} & a_0 x^2 + a_1 x + a_2 \qquad (a_0 \ne 0) \\ & b_0 x^2 + b_1 x + b_2 \qquad (b_0 \ne 0) \end{aligned}$$

have a common root if and only if

$$\begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0 & b_1 & b_2 \end{vmatrix} = 0\ .$$

[*Hint*: Note that if x_1 and x_2 are the roots of the first polynomial, then

$$(x - x_1)(x - x_2) = x^2 + (a_1/a_0)x + a_2/a_0$$

and similarly for the second polynomial.]

8. Show that

$$\begin{vmatrix} x & 0 & 0 & 0 & \cdots & 0 & a_0 \\ -1 & x & 0 & 0 & \cdots & 0 & a_1 \\ 0 & -1 & x & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -1 & a_{n+1} + x \end{vmatrix} = x^n + a_{n-1}x^{n-1} + \cdots + a_0\ .$$

Explain why this shows that given any polynomial $p(x)$ of degree n, there exists a matrix $A \in M_n(\mathcal{F})$ such that $\det(xI - A) = p(x)$. (We will discuss the matrix A in detail in Chapter 8.)

9. Consider the following real matrix:

$$A = \begin{pmatrix} a & b & c & d \\ b & -a & d & -c \\ c & -d & -a & b \\ d & c & -b & -a \end{pmatrix}\ .$$

Show that $\det A = 0$ implies that $a = b = c = d = 0$. [*Hint*: Find AA^T and use Theorems 4.1 and 4.8.]

10. Consider the usual xy-plane $\mathbb{R}^2$. Then the two vectors $x = (x_1, x_2)$ and $y = (y_1, y_2)$ define a quadrilateral with vertices at the points $(0, 0)$, (x_1, x_2), (y_1, y_2) and $(x_1 + y_1, x_2 + y_2)$. Show that (up to a sign) the area of this quadrilateral is given by

$$\begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}\ .$$

[*Hint*: If the vectors x and y are both rotated by an angle θ to obtain the new vectors x′ = (x_1', x_2') and y′ = (y_1', y_2'), then clearly the area of the quadrilateral will remain unchanged. Show (using Example 1.2) it is also true that

$$\begin{vmatrix} x_1' & x_2' \\ y_1' & y_2' \end{vmatrix} = \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}$$

and hence you may choose whatever θ you wish to simplify your calculation.]

What do you think the different signs mean geometrically? We shall have quite a bit more to say on this subject in Chapter 11.

11. Let u, v and w be three vectors in $\mathbb{R}^3$ with the standard inner product, and consider the determinant G(u, v, w) (the **Gramian** of {u, v, w}) defined by

$$G(u,\ v,\ w) = \begin{vmatrix} \langle u,\ u\rangle & \langle u,\ v\rangle & \langle u,\ w\rangle \\ \langle v,\ u\rangle & \langle v,\ v\rangle & \langle v,\ w\rangle \\ \langle w,\ u\rangle & \langle w,\ v\rangle & \langle w,\ w\rangle \end{vmatrix}\ .$$

Show that G(u, v, w) = 0 if and only if {u, v, w} are linearly dependent. As we shall see in Chapter 11, G(u, v, w) represents the volume of the parallelepiped in $\mathbb{R}^3$ defined by {u, v, w}.)

12. Find the inverse (if it exists) of the following matrices:

$(a)\ \begin{pmatrix} 1 & -1 & 2 \\ 1 & 2 & 0 \\ 4 & 1 & 3 \end{pmatrix}$ $\qquad (b)\ \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$(c)\ \begin{pmatrix} -2 & 2 & 3 \\ 4 & 3 & -6 \\ 1 & -1 & 2 \end{pmatrix}$ $\qquad (d)\ \begin{pmatrix} 8 & 2 & 5 \\ -7 & 3 & -4 \\ 9 & -6 & 4 \end{pmatrix}$

$(e)\begin{pmatrix}1 & 2 & 3 & 1\\ 1 & 3 & 3 & 2\\ 2 & 4 & 3 & 3\\ 1 & 1 & 1 & 1\end{pmatrix}$ $(f)\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\\ 3 & 4 & 1 & 2\\ 4 & 1 & 2 & 3\end{pmatrix}$

$(g)\begin{pmatrix}2 & 3 & 2 & 4\\ 4 & 6 & 5 & 5\\ 3 & 5 & 2 & 14\\ 2 & 2 & -3 & 14\end{pmatrix}$

13. Find the inverse of

$$\begin{pmatrix}\cos\theta & -\sin\theta\\ -\sin\theta & -\cos\theta\end{pmatrix}.$$

14. Show that the inverse of the matrix

$$Q = \begin{pmatrix}a_1 & -a_2 & -a_3 & -a_4\\ a_2 & a_1 & -a_4 & a_3\\ a_3 & a_4 & a_1 & -a_2\\ a_4 & -a_3 & a_2 & a_1\end{pmatrix}$$

is given by

$$Q^{-1} = \frac{Q^T}{a_1{}^2 + a_2{}^2 + a_3{}^2 + a_4{}^2}$$

15. Suppose that an n-square matrix A is nilpotent (i.e., $A^k = 0$ for some integer $k > 0$). Prove that $I_n + A$ is nonsingular, and find its inverse. [*Hint*: Note that $(I + A)(I - A) = I - A^2$ etc.]

16. Let $P \in M_n(\mathcal{F})$ be such that $P^2 = P$. If $\lambda \neq 1$, prove that $I_n - \lambda P$ is invertible, and that

$$(I_n - \lambda P)^{-1} = I_n + \frac{\lambda}{1-\lambda}P \ .$$

17. If $A = (a_{ij})$ is a symmetric matrix, show that $(a'_{ij}) = (\text{adj } A)^T$ is also symmetric.

18. If $a, b, c \in \mathbb{R}$, find the inverse of

$$\begin{pmatrix} 1 & a & b \\ -a & 1 & c \\ -b & -c & 1 \end{pmatrix}.$$

19. Prove that Corollary 2 of Theorem 4.3 is valid over a field of characteristic 2. [*Hint*: Use expansion by minors.]

20. (a) Using $A^{-1} = (\text{adj } A)/\det A$, show that the inverse of an upper (lower) triangular matrix is upper (lower) triangular.
(b) If $a \neq 0$, find the inverse of

$$\begin{pmatrix} a & b & c & d \\ 0 & a & b & c \\ 0 & 0 & a & b \\ 0 & 0 & 0 & a \end{pmatrix}.$$

21. Let $A \in M_n(\mathbb{R})$ have all integer entries. Show that the following are equivalent:
(a) $\det A = \pm 1$.
(b) All entries of A^{-1} are integers.

22. For each of the following matrices A, find the value(s) of x for which the **characteristic matrix** $xI - A$ is invertible.

$$(a)\ \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \qquad (b)\ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$(c)\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad (d)\ \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & -1 \end{pmatrix}$$

23. Let $A \in M_n(\mathcal{F})$ have exactly one nonzero entry in each row and column. Show that A is invertible, and that its inverse is of the same form.

24. If $A \in M_n(\mathcal{F})$, show that $\det(\text{adj } A) = (\det A)^{n-1}$.

25. Show that A is nonsingular if and only if adj A is nonsingular.

26. Using determinants, find the rank of each of the following matrices:

$$(a)\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ -1 & 2 & 1 & 0 \end{pmatrix}$$

$$(b)\ \begin{pmatrix} -1 & 0 & 1 & 2 \\ 1 & 1 & 3 & 0 \\ -1 & 2 & 4 & 1 \end{pmatrix}$$

4.4 DETERMINANTS AND LINEAR EQUATIONS

Suppose that we have a system of n equations in n unknowns which we write in the usual way as

$$\sum_{j=1}^{n} a_{ij}x_j = b_i\ , \qquad i = 1, \dots, n\ .$$

We assume that $A = (a_{ij}) \in M_n(\mathcal{F})$ is nonsingular. In matrix form, this system may be written as AX = B as we saw earlier. Since A is nonsingular, A^{-1} exists (Theorem 3.21) and det A ≠ 0 (Theorem 4.6). Therefore the solution to AX = B is given by

$$X = A^{-1}B = \frac{(\operatorname{adj} A)B}{\det A}\ .$$

But $\operatorname{adj} A = (a'_{ij})^T$ so that

$$x_j = \sum_{i=1}^{n} \frac{(\operatorname{adj} A)_{ji} b_i}{\det A} = \sum_{i=1}^{n} \frac{a'_{ij} b_i}{\det A}\ .$$

From Corollary 1 of Theorem 4.10, we see that $\sum_i b_i a'_{ij}$ is just the expansion by minors of the *jth* column of the matrix C whose columns are given by $C^i = A^i$ for i ≠ j and $C^j = B$. We are thus led to the following result, called **Cramer's rule**.

Theorem 4.13 If $A = (a_{ij}) \in M_n(\mathcal{F})$ is nonsingular, then the system of linear equations

$$\sum_{j=1}^{n} a_{ij}x_j = b_i\ , \qquad i = 1, \dots, n$$

has the unique solution

$$x_j = \frac{1}{\det A}\det(A^1, \dots, A^{j-1}, B, A^{j+1}, \dots, A^n)\ .$$

Proof This theorem was actually proved in the preceding discussion, where uniqueness follows from Theorem 3.16. However, it is instructive to give a more direct proof as follows. We write our system as $\Sigma A^i x_i = B$ and simply compute using Corollary 1 of Theorem 4.2 and Corollary 2 of Theorem 4.3:

$$\begin{aligned}\det(A^1, \dots, A^{j-1}, B, A^{j+1}, \dots, A^n) &= \det(A^1, \dots, A^{j-1}, \Sigma A^i x_i, A^{j+1}, \dots, A^n)\\ &= \Sigma x_i \det(A^1, \dots, A^{j-1}, A^i, A^{j+1}, \dots, A^n)\\ &= x_j \det(A^1, \dots, A^{j-1}, A^j, A^{j+1}, \dots, A^n)\\ &= x_j \det A \ . \ ∎\end{aligned}$$

Corollary A homogeneous system of equations

$$\sum_{j=1}^{n} a_{ij}x_j = 0 \ , \qquad i = 1, \dots, n$$

has a nontrivial solution if and only if $\det A = 0$.

Proof We see from Cramer's rule that if $\det A \neq 0$, then the solution of the homogeneous system is just the zero vector (by Corollary 2 of Theorem 4.2 as applied to columns instead of rows). This shows that the if the system has a nontrivial solution, then $\det A = 0$.

On the other hand, if $\det A = 0$ then the columns of A must be linearly dependent (Theorem 4.6). But the system $\Sigma_j a_{ij} x_j = 0$ may be written as $\Sigma_j A^j x_j = 0$ where A^j is the *jth* column of A. Hence the linear dependence of the A^j shows that the x_j may be chosen such that they are not all zero, and therefore a nontrivial solution exists. (We remark that this corollary also follows directly from Theorems 3.12 and 4.6.) ∎

Example 4.6 Let us solve the system

$$\begin{aligned}5x + 2y + \ \ z &= 3\\ 2x - \ \ y + 2z &= 7\\ x + 5y - \ \ z &= 6\end{aligned}$$

We see that $A = (a_{ij})$ is nonsingular since

$$\begin{vmatrix} 5 & 2 & 1 \\ 2 & -1 & 2 \\ 1 & 5 & -1 \end{vmatrix} = -26 \neq 0 \ .$$

We then have

$$x = \frac{-1}{26}\begin{vmatrix} 3 & 2 & 1 \\ 7 & -1 & 2 \\ 6 & 5 & -1 \end{vmatrix} = (-1/26)(52) = -2$$

$$y = \frac{-1}{26}\begin{vmatrix} 5 & 3 & 1 \\ 2 & 7 & 2 \\ 1 & 6 & -1 \end{vmatrix} = (-1/26)(-78) = 3$$

$$z = \frac{-1}{26}\begin{vmatrix} 5 & 2 & 3 \\ 2 & -1 & 7 \\ 1 & 5 & 6 \end{vmatrix} = (-1/26)(-182) = 7 \ . \quad /\!\!/$$

Exercises

1. Using Cramer's rule, find a solution (if it exists) of the following systems of equations:

(*a*)
$$\begin{aligned} 3x + y - z &= 0 \\ x - y + 3z &= 1 \\ 2x + 2y + z &= 7 \end{aligned}$$

(*b*)
$$\begin{aligned} 2x + y + 2z &= 0 \\ 3x - 2y + z &= 1 \\ -x + 2y + 2z &= -7 \end{aligned}$$

(*c*)
$$\begin{aligned} 2x - 3y + z &= 10 \\ -x + 3y + 2z &= -2 \\ 4x + 4y + 5z &= 4 \end{aligned}$$

(*d*)
$$\begin{aligned} x + 2y - 3z + t &= -9 \\ 2x + y + 2z - t &= 3 \\ -x + y + 2z - t &= 0 \\ 3x + 4y + z + 4t &= 3 \end{aligned}$$

2. By calculating the inverse of the matrix of coefficients, solve the following systems:

(*a*)
$$\begin{aligned} 2x - 3y + z &= a \\ x + 2y + 3z &= b \\ 3x - y + 2z &= c \end{aligned}$$

(*b*)
$$\begin{aligned} x + 2y + 4z &= a \\ -x + 3y - 2z &= b \\ 2x - y + z &= c \end{aligned}$$

$$(c)\ \begin{aligned} 2x + y + 2z - 3t &= a \\ 3x + 2y + 3z - 5t &= b \\ 2x + 2y + z - t &= c \\ 5x + 5y + 2z - 2t &= d \end{aligned} \qquad (d)\ \begin{aligned} 6x + y + 4z - 3t &= a \\ 2x - y &= b \\ x + y + z &= c \\ -3x - y - 2z + t &= d \end{aligned}$$

3. If det A ≠ 0 and AB = AC, show that B = C.

4. Find, if possible, a 2 x 2 matrix X that satisfies each of the given equations:

$$(a)\ \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} X \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$(b)\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} X \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$$

5. Consider the system

$$\begin{aligned} ax + by &= \alpha + \beta t \\ cx + dy &= \gamma + \delta t \end{aligned}$$

where t is a parameter, $\beta^2 + \delta^2 \neq 0$ and

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0 \ .$$

Show that the set of solutions as t varies is a straight line in the direction of the vector

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \beta \\ \delta \end{pmatrix} \ .$$

6. Let A, B, C and D be 2 x 2 matrices, and let R and S be vectors (i.e., 2 x 1 matrices). Show that the system

$$\begin{aligned} AX + BY &= R \\ CX + DY &= S \end{aligned}$$

can always be solved for vectors X and Y if

$$\begin{vmatrix} a_{11} & a_{12} & b_{11} & b_{12} \\ a_{21} & a_{22} & b_{21} & b_{22} \\ c_{11} & c_{12} & d_{11} & d_{12} \\ c_{21} & c_{22} & d_{21} & d_{22} \end{vmatrix} \neq 0 \ .$$

4.5 BLOCK MATRICES

There is another definition that will greatly facilitate our discussion of matrix representations of operators to be presented in Chapter 7. In particular, suppose that we are given a matrix $A = (a_{ij}) \in M_{m\mathrm{x}n}(\mathcal{F})$. Then, by partitioning the rows and columns of A in some manner, we obtain what is called a **block matrix**. To illustrate, suppose $A \in M_{3\mathrm{x}5}(\mathbb{R})$ is given by

$$A = \begin{pmatrix} 7 & 5 & 5 & 4 & -1 \\ 2 & 1 & -3 & 0 & 5 \\ 0 & 8 & 2 & 1 & -9 \end{pmatrix} \ .$$

Then we may partition A into blocks to obtain (for example) the matrix

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

where

$$A_{11} = \begin{pmatrix} 7 & 5 & 5 \end{pmatrix} \qquad A_{12} = \begin{pmatrix} 4 & -1 \end{pmatrix}$$

$$A_{21} = \begin{pmatrix} 2 & 1 & -3 \\ 0 & 8 & 2 \end{pmatrix} \qquad A_{22} = \begin{pmatrix} 0 & 5 \\ 1 & -9 \end{pmatrix}$$

(do not confuse these A_{ij} with minor matrices).

If A and B are block matrices that are partitioned into the same number of blocks such that each of the corresponding blocks is of the same size, then it is clear that (in an obvious notation)

$$A + B = \begin{pmatrix} A_{11} + B_{11} & \cdots & A_{1n} + B_{1n} \\ \vdots & & \vdots \\ A_{m1} + B_{m1} & \cdots & A_{mn} + B_{mn} \end{pmatrix} \ .$$

In addition, if C and D are block matrices such that the number of columns in each C_{ij} is equal to the number of rows in each D_{jk}, then the product of C and D is also a block matrix CD where $(CD)_{ik} = \sum_j C_{ij} D_{jk}$. Thus block matrices are multiplied as if each block were just a single element of each matrix in the product. In other words, each $(CD)_{i\,k}$ is a matrix that is the sum of a product of matrices. The proof of this fact is an exercise in matrix multiplication, and is left to the reader (see Exercise 4.5.1).

Theorem 4.14 If $A \in M_n(\mathcal{F})$ is a block triangular matrix of the form

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} & \cdots & A_{1k} \\ 0 & A_{22} & A_{23} & \cdots & A_{2k} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & A_{kk} \end{pmatrix}$$

where each A_{ii} is a square matrix and the 0's are zero matrices of appropriate size, then

$$\det A = \prod_{i=1}^{k} \det A_{ii} \quad .$$

Proof What is probably the simplest proof of this theorem is outlined in Exercise 4.5.3. However, the proof that follows serves as a good illustration of the meaning of the terms in the definition of the determinant. We first note that only the diagonal matrices are required to be square matrices. Because each A_{ii} is square, we can simply prove the theorem for the case $k = 2$, and the general case will then follow by induction. We thus let $A = (a_{ij}) \in M_n(\mathcal{F})$ be of the form

$$\begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

where $B = (b_{ij}) \in M_r(\mathcal{F})$, $D = (d_{ij}) \in M_s(\mathcal{F})$, $C = (c_{ij}) \in M_{r\text{x}s}(\mathcal{F})$ and $r + s = n$. Note that for $1 \le i, j \le r$ we have $a_{ij} = b_{ij}$, for $1 \le i, j \le s$ we have $a_{i+r\, j+r} = d_{ij}$, and if $i > r$ and $j \le r$ then $a_{ij} = 0$. From the definition of determinant we have

$$\det A = \Sigma_{\sigma\in S_n} (\operatorname{sgn}\sigma) a_{1\,\sigma 1} \cdots a_{r\,\sigma r} a_{r+1\,\sigma(r+1)} \cdots a_{n\,\sigma n} \quad .$$

By definition, each $\sigma \in S_n$ is just a rearrangement (i.e., permutation) of the n elements in S_n. This means that for each $\sigma \in S_n$ with the property that $\sigma i > r$ for some $i \le r$, there must be some $i' > r$ such that $\sigma i' \le r$. Then for this i' we have $a_{i'\sigma i'} = 0$, and hence each term in det A that contains one of these factors is zero. Therefore each nonzero term in the above sum must be over only those permutations σ such that $\sigma i > r$ if $i > r$ (i.e., the block D), and $\sigma i \le r$ if $i \le r$ (i.e., the block B).

To separate the action of the allowed σ on the blocks B and D, we define the permutations $\alpha \in S_r$ and $\beta \in S_s$ by $\alpha i = \sigma i$ for $1 \le i \le r$, and $\beta i = \sigma(i + r) - r$ for $1 \le i \le s$. In other words, each of the allowed σ is just some rearrangement α of the values of i for $1 \le i \le r$ along with some rearrangement β of the values of i for $r < i \le r + s = n$, and there is no mixing between these blocks. The permutations α and β are thus independent, and since sgn σ is defined by the number of transpositions involved, this number simply separates into the number of transpositions in α plus the number of transpositions in β. Therefore sgn σ = (sgn α)(sgn β).

The result of this is that all nonzero terms in det A are of the form

$$(\operatorname{sgn}\alpha)b_{1\,\alpha 1} \cdots b_{r\,\alpha r}(\operatorname{sgn}\beta)d_{1\,\beta 1} \cdots d_{s\,\beta s} \;\; .$$

Furthermore, every term of this form is included in the expression for det A, and hence det A = (det B)(det D). ∎

There is another way to prove this theorem that is based on our earlier formula

$$D(A) = (\det A)D(I) \qquad (2)$$

where D is any multilinear and alternating function on the set of all n x n matrices (see the discussion following the proof of Theorem 4.9). To show this, consider the block triangular matrix

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

where A and C are square matrices. Suppose we define the function

$$D(A,\, B,\, C) = \begin{vmatrix} A & B \\ 0 & C \end{vmatrix} \;\; .$$

If we consider the matrices A and B to be fixed, then this is clearly a multilinear and alternating function of the rows of C. Applying equation (2), this may be written as

$$D(A, B, C) \;=\; (\det C)\, D(A, B, I)$$

where

$$D(A,\, B,\, I) = \begin{vmatrix} A & B \\ 0 & I \end{vmatrix} \;\; .$$

But using Theorem 4.4(c) it should be obvious that we can subtract suitable multiples of the rows of I from the matrix B so that

$$D(A, B, I) = D(A, 0, I) .$$

Applying the same reasoning, we observe that D(A, 0, I) is a multilinear and alternating function of the rows of A, and hence (2) again yields

$$D(A, 0, I) = (\det A)\, D(I, 0, I) .$$

Putting all of this together along with the obvious fact that D(I, 0, I) = 1, we obtain

$$\begin{aligned} D(A, B, C) &= (\det C) D(A, B, I) \\ &= (\det C) D(A, 0, I) \\ &= (\det C)(\det A) D(I, 0, I) \\ &= (\det C)(\det A) \end{aligned}$$

which agrees with Theorem 4.14.

Example 4.7 Consider the matrix

$$A = \begin{pmatrix} 1 & -1 & 2 & 3 \\ 2 & 2 & 0 & 2 \\ 4 & 1 & -1 & -1 \\ 1 & 2 & 3 & 0 \end{pmatrix} .$$

By the addition of suitable multiples of one row to another, it is easy to row-reduce A to the form

$$B = \left(\begin{array}{cc} \boxed{\begin{matrix} 1 & -1 \\ 0 & 4 \end{matrix}} & \boxed{\begin{matrix} 2 & 3 \\ -4 & -4 \end{matrix}} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \boxed{\begin{matrix} -4 & -8 \\ 4 & 0 \end{matrix}} \end{array}\right)$$

with det B = det A. Since B is in block triangular form we have

$$\det A = \det B = \begin{vmatrix} 1 & -1 \\ 0 & 4 \end{vmatrix} \begin{vmatrix} -4 & -8 \\ 4 & 0 \end{vmatrix} = 4(32) = 128 \quad . \quad /\!\!/$$

Exercises

1. Prove the multiplication formula given in the text (just prior to Theorem 4.14) for block matrices.

2. Suppose $A \in M_n(\mathcal{F})$, $D \in M_m(\mathcal{F})$, $U \in M_{n\mathrm{x}m}(\mathcal{F})$ and $V \in M_{m\mathrm{x}n}(\mathcal{F})$, and consider the (n + m) x (n + m) matrix

$$M = \begin{pmatrix} A & U \\ V & D \end{pmatrix} \; .$$

If A^{-1} exists, show that

$$\begin{pmatrix} A^{-1} & 0 \\ -VA^{-1} & I_m \end{pmatrix}\begin{pmatrix} A & U \\ V & D \end{pmatrix} = \begin{pmatrix} I_n & A^{-1}U \\ 0 & -VA^{-1}U + D \end{pmatrix}$$

and hence that

$$\begin{vmatrix} A & U \\ V & D \end{vmatrix} = (\det A)\det(D - VA^{-1}U) \; .$$

3. Let A be a block triangular matrix of the form

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

where B and D are square matrices. Prove det A = (det B)(det D) by using elementary row operations on A to create a block triangular matrix

$$\tilde{A} = \begin{pmatrix} \tilde{B} & \tilde{C} \\ 0 & \tilde{D} \end{pmatrix}$$

where $\tilde{B}$ and $\tilde{D}$ are upper-triangular.

4. Show

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^T = \begin{pmatrix} A^T & C^T \\ B^T & D^T \end{pmatrix} \; .$$

4.6 THE CAUCHY-BINET THEOREM

This section deals with a generalization of Theorem 4.8 that is not used anywhere in this book except in Chapter 8. Because of this, the reader should feel free to skip this section now and come back to it if and when it is needed. Let us first point out that while Theorem 4.8 dealt with the product of square matrices, it is nevertheless possible to formulate a similar result even in the case where $A \in M_{n\text{x}p}(\mathcal{F})$ and $B \in M_{p\text{x}n}(\mathcal{F})$ (so that the product $AB \in M_n(\mathcal{F})$ is square and det AB is defined). This result is the main subject of this section, and is known as the Cauchy-Binet theorem.

Before proceeding with our discussion, we briefly present some new notation that will simplify some of our formulas significantly, although at first it may seem that all we are doing is complicating things needlessly. Suppose that we have a matrix A with m rows and n columns. Then we can easily form a new matrix B by considering only those elements of A belonging to, say, rows 2 and 3 and columns 1, 3 and 4. We shall denote this **submatrix** B of A by $B = A[2, 3|1, 3, 4]$. What we now wish to do is make this definition precise.

To begin with, let k and n be positive integers with $1 \leq k \leq n$. We let MAP(k, n) denote the set of *all* mappings from the set $\underline{k} = (1, \dots, k)$ to the set $\underline{n} = (1, \dots, n)$. For example, if $n = 5$ and $k = 3$, we can define $\alpha \in \text{MAP}(3, 5)$ by $\alpha(1) = 2$, $\alpha(2) = 5$ and $\alpha(3) = 3$. Note that an arbitrary $\alpha \in \text{MAP}(k, n)$ need not be injective so that, for example, $\alpha' \in \text{MAP}(3, 5)$ could be defined by $\alpha'(1) = 2$, $\alpha'(2) = 5$ and $\alpha'(3) = 5$. In fact, we will let INC(k, n) denote the set of all *strictly increasing* functions from the set $\underline{k}$ into the set $\underline{n}$. Thus if $\beta \in$ INC(k, n), then $\beta(1) < \beta(2) < \cdots < \beta(k)$. We also denote the mapping β by simply the k-tuple of numbers $\beta = (\beta(1), \dots, \beta(k))$. Note that this k-tuple consists of k distinct integers in increasing order.

Now consider the set of all possible permutations of the k integers within each k-tuple β for every $\beta \in \text{INC}(k, n)$. This yields the set INJ(k, n) consisting of all injective mappings from the set $\underline{k}$ into the set $\underline{n}$. In other words, if $\beta \in$ INJ(k, n), then $\beta = (\beta(1), \dots, \beta(k))$ is a k-tuple of k distinct integers in any (i.e., not necessarily increasing) order. In the particular case that $k = n$, we see that the set INJ(n, n) is just the set of all permutations of the integers $1, \dots, n$. The set INJ(n, n) will be denoted by PER(n). (Note that the set INJ(n, n) is the same as the set S_n, but without the additional group structure.)

Now suppose that $A = (a_{ij}) \in M_{m\text{x}n}(\mathcal{F})$, let $\alpha = (i_1, \dots, i_k) \in \text{INC}(k, m)$ and let $\beta = (j_1, \dots, j_t) \in \text{INC}(t, n)$. Then the matrix $B \in M_{k\text{x}t}(\mathcal{F})$ whose (r, s)*th* entry is $a_{i_r j_s}$ (where $1 \leq r \leq k$ and $1 \leq s \leq t$) is called the **submatrix** of A lying in rows α and columns β. We will denote this submatrix by $A[\alpha|\beta]$. Similarly, we let $A(\alpha|\beta] \in M_{(m-k)\text{x}t}(\mathcal{F})$ denote the submatrix of A whose rows are precisely those *complementary* to α, and whose columns are again given by β. It should be clear that we can analogously define the matrices $A(\alpha|\beta) \in M_{(m-k)\text{x}(n-t)}(\mathcal{F})$ and $A[\alpha|\beta) \in M_{k\text{x}(n-t)}(\mathcal{F})$. Fortunately, these ideas are more difficult to state carefully than they are to understand. Hopefully the next example should clarify everything.

Example 4.8 Suppose A ∈ $M_{5x6}(\mathcal{F})$, and let α = (1, 3) ∈ INC(2, 5) and β = (2, 3, 4) ∈ INC(3, 6). Then

$$A[\alpha \mid \beta] = \begin{pmatrix} a_{12} & a_{13} & a_{14} \\ a_{32} & a_{33} & a_{34} \end{pmatrix} \qquad A[\alpha \mid \beta) = \begin{pmatrix} a_{11} & a_{15} & a_{16} \\ a_{31} & a_{35} & a_{36} \end{pmatrix}$$

$$A(\alpha \mid \beta] = \begin{pmatrix} a_{22} & a_{23} & a_{24} \\ a_{42} & a_{43} & a_{44} \\ a_{52} & a_{53} & a_{54} \end{pmatrix} \qquad A(\alpha \mid \beta) = \begin{pmatrix} a_{21} & a_{25} & a_{26} \\ a_{41} & a_{45} & a_{46} \\ a_{51} & a_{55} & a_{56} \end{pmatrix} . \quad /\!\!/$$

Before stating and proving the main result of this section, it will be useful for us to gather together several elementary computational facts that we will need.

Lemma 4.1

$$\prod_{i=1}^{k}\left(\sum_{j=1}^{n} x_{ij}\right) = \sum_{\alpha \in MAP(k,\, n)} \left(\prod_{i=1}^{k} x_{i\ \alpha(i)}\right) .$$

To see that this is true, we simply look at a particular example. Thus, consider the set MAP(2, 3). This consists of all mappings α such that α(i) ∈ $\underline{3}$ for each i = 1, 2. It is easy to enumerate all nine possibilities:

$$\begin{aligned} &\alpha(1) = 1 \quad \text{and} \quad \alpha(2) = 1,\ 2,\ \text{or}\ 3 \\ &\alpha(1) = 2 \quad \text{and} \quad \alpha(2) = 1,\ 2,\ \text{or}\ 3 \\ &\alpha(1) = 3 \quad \text{and} \quad \alpha(2) = 1,\ 2,\ \text{or}\ 3 \end{aligned}$$

Expanding the product in the natural way we obtain

$$\begin{aligned} \prod_{i=1}^{2}\left(\sum_{j=1}^{3} x_{ij}\right) &= (x_{11} + x_{12} + x_{13})(x_{21} + x_{22} + x_{23}) \\ &= x_{11}x_{21} + x_{11}x_{22} + x_{11}x_{23} + x_{12}x_{21} + x_{12}x_{22} \\ &\qquad + x_{12}x_{23} + x_{13}x_{21} + x_{13}x_{22} + x_{13}x_{23} \\ &= \sum_{\alpha \in MAP(2,\, 3)} x_{1\ \alpha(1)} x_{2\ \alpha(2)} \\ &= \sum_{\alpha \in MAP(2,\, 3)} \left(\prod_{i=1}^{2} x_{i\ \alpha(i)}\right) . \end{aligned}$$

A minutes thought should convince the reader that Lemma 4.1 is true in general. If it does not, then pick an example and work it out for yourself.

Recall from Section 4.1 that we may view the determinant as a function of either the rows A_i or columns A^i of a matrix $A \in M_n(\mathcal{F})$. Applying the definition of determinant and Corollary 2 of Theorem 4.3, we obtain the next fact. Note that even though we originally defined $A[\alpha|\beta]$ for $\alpha, \beta \in$ INC(m, n), we can just as well assume that $\alpha, \beta \in$ MAP(m, n).

Lemma 4.2 If $\alpha = (\alpha(1), \dots, \alpha(n)) \in$ MAP(n, n) is *not* an injection, then for any square matrix $A = (a_{ij}) \in M_n(\mathcal{F})$ we have

$$\det A[\alpha \mid \underline{n}] = \sum_{\theta \in PER(n)} (\operatorname{sgn} \theta) \prod_{i=1}^{n} a_{\alpha(i)\theta(i)} = 0\ .$$

Our discussion above showed that the set INJ(k, n) arose by considering all permutations of the k-tuples in INC(k, n). Let us take a closer look at the consequences of this observation. If $(\alpha(1), \dots, \alpha(k)) \in$ INJ(k , n), then there are n choices for $\alpha(1)$, n - 1 choices for $\alpha(2)$ and so on down to n - (k - 1) choices for $\alpha(k)$. In other words, the set INJ(k, n) consists of

$$n(n - 1) \cdots (n - (k - 1)) = n!/(n - k)!$$

mappings. It should also be clear that the set INC(k, n) consists of $\binom{n}{k}$ = n!/[k!(n - k)!] mappings since INC(k, n) is just the collection of increasing k-tuples taken from the set $\underline{n}$. Finally, we recall that PER(k) has k! elements, and therefore we see that the number of elements in INJ(k, n) is just the number of elements in INC(k, n) times the number of elements in PER(k).

As an example, let n = 4 and k = 3. Then INC(3, 4) consists of the sequences (1, 2, 3), (1, 2, 4), (1, 3, 4) and (2, 3, 4). If we enumerate all possible permutations of each of these, we obtain the following elements of INJ(3, 4):

123	124	134	234
132	142	143	243
213	214	314	324
231	241	341	342
312	412	413	423
321	421	431	432

In the next lemma, we let Q_α be some quantity that depends on the mapping α, and let $\alpha\theta$ denote the composition of α and θ.

Lemma 4.3

$$\sum_{\alpha\in INJ(k,\,n)} Q_\alpha = \sum_{\alpha\in INC(k,\,n)}\ \sum_{\theta\in PER(k)} Q_{\alpha\theta}\ .$$

A careful look at the above example should make this fact obvious. Note that it is not so much a statement about sums as it is about the set INJ(k, n).

Finally, our last fact is just a restatement of Theorem 4.3 in our current notation.

Lemma 4.4 Let $A \in M_{m\mathrm{x}n}(\mathcal{F})$ where $m \geq n$, and suppose that $\theta \in PER(n)$ and $\alpha \in MAP(n, m)$. Then

$$\det A[\alpha\theta|\underline{n}\,] = (\operatorname{sgn}\theta)\det A[\alpha|\underline{n}\,]\ .$$

We are now in a position to state and prove the main result needed for the Cauchy-Binet theorem. Note in the following that the particular case of n = p is just Theorem 4.8.

Theorem 4.15 Suppose $A = (a_{ij}) \in M_{n\mathrm{x}p}(\mathcal{F})$ and $B = (b_{ij}) \in M_{p\mathrm{x}n}(\mathcal{F})$ where $n \leq p$. Then

$$\det(AB) = \sum_{\alpha\in INC(n,\,p)} (\det A[\underline{n}\mid\alpha])(\det B[\alpha\mid\underline{n}])$$

Proof From the definitions of determinant and matrix product we have

$$\begin{aligned}\det(AB) &= \sum_{\theta\in PER(n)} (\operatorname{sgn}\theta)\prod_{i=1}^{n}(AB)_{i\ \theta(i)}\\ &= \sum_{\theta\in PER(n)} (\operatorname{sgn}\theta)\left(\prod_{i=1}^{n}\sum_{j=1}^{p} a_{ij}b_{j\ \theta(i)}\right)\ .\end{aligned}$$

Using Lemma 4.1 with $x_{ij} = a_{ij}b_{j\theta(i)}$ the right hand side of this expression becomes

$$\sum_{\theta \in PER(n)} (\operatorname{sgn} \theta)\left(\sum_{\alpha \in MAP(n,\ p)} \prod_{i=1}^{n} a_{i\ \alpha(i)} b_{\alpha(i)\ \theta(i)} \right)$$

$$= \sum_{\alpha \in MAP(n,\ p)} \left\{ \left(\prod_{i=1}^{n} a_{i\ \alpha(i)} \right) \left(\sum_{\theta \in PER(n)} (\operatorname{sgn} \theta) \prod_{i=1}^{n} b_{\alpha(i)\ \theta(i)} \right) \right\}$$

$$= \sum_{\alpha \in MAP(n,\ p)} \left\{ \left(\prod_{i=1}^{n} a_{i\ \alpha(i)} \right) \det B[\alpha \mid \underline{n}] \right\} .$$

By Lemma 4.2, we need only sum over those α ∈ INJ(n, p). Combining this with Lemma 4.3 we obtain for this last expression

$$\sum_{\alpha \in INC(n,\ p)} \sum_{\theta \in PER(n)} \left(\det B[\alpha\theta \mid \underline{n}] \prod_{i=1}^{n} a_{i\ \alpha\theta(i)} \right) .$$

Now, applying Lemma 4.4, this becomes

$$\sum_{\alpha \in INC(n,\ p)} \det B[\alpha \mid \underline{n}] \left(\sum_{\theta \in PER(n)} (\operatorname{sgn} \theta) \prod_{i=1}^{n} a_{i\ \alpha\theta(i)} \right)$$

$$= \sum_{\alpha \in INC(n,\ p)} (\det B[\alpha \mid \underline{n}])(\det A[\underline{n} \mid \alpha]) .$$

This completes the proof. ∎

Note the particular case of p = n yields an independent proof of Theorem 4.8.

The principal result of this section now follows as an easy generalization of Theorem 4.15. Thus, suppose that $A \in M_{n\times s}(\mathcal{F})$ and $B \in M_{s\times m}(\mathcal{F})$, and let $1 \le r \le \min\{n, s, m\}$. If $\alpha \in INC(r, n)$ and $\beta \in INC(r, m)$, we have

$$C = AB = \begin{pmatrix} A_1B^1 & \cdots & A_1B^m \\ \vdots & & \vdots \\ A_nB^1 & \cdots & A_nB^m \end{pmatrix}$$

and

$$C[\alpha \mid \beta] = \begin{pmatrix} A_{\alpha_1}B^{\beta_1} & \cdots & A_{\alpha_1}B^{\beta_r} \\ \vdots & & \vdots \\ A_{\alpha_r}B^{\beta_1} & \cdots & A_{\alpha_r}B^{\beta_r} \end{pmatrix} .$$

Then $C[\alpha|\beta] = A[\alpha|\,\underline{s}]\, B[\underline{s}|\beta] \in M_r(\mathcal{F})$ and we can now apply Theorem 4.15 to obtain the following corollary, known as the Cauchy-Binet theorem.

Corollary (Cauchy-Binet) Suppose $A \in M_{n\mathrm{x}s}(\mathcal{F})$, $B \in M_{s\mathrm{x}m}(\mathcal{F})$ and $C = AB$. Then for any r with $1 \le r \le \min\{n, s, m\}$ and $\alpha \in \mathrm{INC}(r, n)$, $\beta \in \mathrm{INC}(r, m)$ we have

$$\det C[\alpha \mid \beta] = \sum_{\omega \in INC(r,\, s)} (\det A[\alpha \mid \omega])(\det B[\omega \mid \beta]) \ .$$

Example 4.9 Let

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} .$$

The increasing functions from $\underline{2}$ to $\underline{3}$ are (1, 2), (1, 3) and (2, 3), and hence

$$A[\underline{2} \mid 1, 2] = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad A[\underline{2} \mid 1, 3] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A[\underline{2} \mid 2, 3] = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad B[1, 2 \mid \underline{2}] = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$B[1, 3 \mid \underline{2}] = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \qquad B[2, 3 \mid \underline{2}] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Applying Theorem 4.15 we have

$$\begin{aligned} \det AB &= \det A[\underline{2} \mid 1, 2] \det B[1, 2 \mid \underline{2}] + \det A[\underline{2} \mid 1, 3] \det B[1, 3 \mid \underline{2}] \\ &\qquad + \det A[\underline{2} \mid 2, 3] \det B[2, 3 \mid \underline{2}] \\ &= (1)(-1) + (1)(-1) + (1)(-1) \\ &= -3 \ . \end{aligned}$$

We leave it to the reader to verify that directly evaluating the product AB and taking its determinant yields the same result. //

CHAPTER 5

Linear Transformations and Matrices

In Section 3.1 we defined matrices by systems of linear equations, and in Section 3.6 we showed that the set of all matrices over a field $\mathcal{F}$ may be endowed with certain algebraic properties such as addition and multiplication. In this chapter we present another approach to defining matrices, and we will see that it also leads to the same algebraic behavior as well as yielding important new properties.

5.1 LINEAR TRANSFORMATIONS

Recall that vector space homomorphisms were defined in Section 2.2. We now repeat that definition using some new terminology. In particular, a mapping T: U → V of two vector spaces over the same field $\mathcal{F}$ is called a **linear transformation** if it has the following properties for all x, y ∈ U and a ∈ $\mathcal{F}$:

(a) $T(x + y) = T(x) + T(y)$
(b) $T(ax) = aT(x)$.

Letting a = 0 and −1 shows

$$T(0) = 0$$

and

$$T(-x) = -T(x) .$$

We also see that

$$T(x - y) = T(x + (-y)) = T(x) + T(-y) = T(x) - T(y) .$$

It should also be clear that by induction we have, for any finite sum,

$$T(\Sigma a_i x_i) = \Sigma T(a_i x_i) = \Sigma a_i T(x_i)$$

for any vectors $x_i \in V$ and scalars $a_i \in \mathcal{F}$.

Example 5.1 Let T: $\mathbb{R}^3 \rightarrow \mathbb{R}^2$ be the "projection" mapping defined for any $u = (x, y, z) \in \mathbb{R}^3$ by

$$T(u) = T(x, y, z) = (x, y, 0) .$$

Then if $v = (x', y', z')$ we have

$$\begin{aligned} T(u+v) &= T(x+x',\ y+y',\ z+z') \\ &= (x+x',\ y+y',\ 0) \\ &= (x,\ y,\ 0) + (x',\ y',\ 0) \\ &= T(u) + T(v) \end{aligned}$$

and

$$T(au) = T(ax, ay, az) = (ax, ay, 0) = a(x, y, 0) = aT(u) .$$

Hence T is a linear transformation. ∕∕

Example 5.2 Let $P \in M_n(\mathcal{F})$ be a fixed invertible matrix. We define a mapping $S: M_n(\mathcal{F}) \rightarrow M_n(\mathcal{F})$ by $S(A) = P^{-1}AP$. It is easy to see that this defines a linear transformation since

$$S(\alpha A + B) = P^{-1}(\alpha A + B)P = \alpha P^{-1}AP + P^{-1}BP = \alpha S(A) + S(B) . \ /\!/$$

Example 5.3 Let V be a real inner product space, and let W be any subspace of V. By Theorem 2.22 we have $V = W \oplus W^\perp$, and hence by Theorem 2.12, any $v \in V$ has a unique decomposition $v = x + y$ where $x \in W$ and $y \in W^\perp$. Now define the mapping $T: V \rightarrow W$ by $T(v) = x$. Then

$$T(v_1 + v_2) = x_1 + x_2 = T(v_1) + T(v_2)$$

and

$$T(av) = ax = aT(v)$$

so that T is a linear transformation. This mapping is called the **orthogonal projection** of V onto W. ⫽

Let T: V → W be a linear transformation, and let $\{e_i\}$ be a basis for V. Then for any x ∈ V we have $x = \sum x_ie_i$, and hence

$$T(x) = T(\sum x_ie_i) = \sum x_iT(e_i) \;.$$

Therefore, if we know all of the $T(e_i)$, then we know T(x) for any x ∈ V. In other words, *a linear transformation is determined by specifying its values on a basis.* Our first theorem formalizes this fundamental observation.

Theorem 5.1 Let U and V be finite-dimensional vector spaces over $\mathcal{F}$, and let $\{e_1, \dots, e_n\}$ be a basis for U. If $v_1, \dots, v_n$ are any n arbitrary vectors in V, then there exists a unique linear transformation T: U → V such that $T(e_i) = v_i$ for each i = 1, . . . , n.

Proof For any x ∈ U we have $x = \sum_{i=1}^n x_ie_i$ for some unique set of scalars x_i (Theorem 2.4, Corollary 2). We define the mapping T by

$$T(x) = \sum_{i=1}^n x_iv_i$$

for any x ∈ U. Since the x_i are unique, this mapping is well-defined (see Exercise 5.1.1). Noting that for any i = 1, . . . , n we have $e_i = \sum_j \delta_{ij}e_j$, it follows that

$$T(e_i) = \sum_{j=1}^n \delta_{ij}v_j = v_i \;.$$

We show that T so defined is a linear transformation.

If $x = \sum x_ie_i$ and $y = \sum y_ie_i$, then $x + y = \sum(x_i + y_i)e_i$, and hence

$$T(x + y) = \sum(x_i + y_i)v_i = \sum x_iv_i + \sum y_iv_i = T(x) + T(y) \;.$$

Also, if $c \in \mathcal{F}$ then $cx = \sum(cx_i)e_i$, and thus

$$T(cx) = \sum(cx_i)v_i = c\sum x_iv_i = cT(u)$$

which shows that T is indeed a linear transformation.

Now suppose that T′: U → V is any other linear transformation defined by $T'(e_i) = v_i$. Then for any x ∈ U we have

$$T'(x) = T'(\sum x_ie_i) = \sum x_iT'(e_i) = \sum x_iv_i = \sum x_iT(e_i) = T(\sum x_ie_i) = T(x)$$

and hence $T'(x) = T(x)$ for all $x \in U$. This means that $T' = T$ which thus proves uniqueness. ∎

Example 5.4 Let $T \in L(\mathcal{F}^m, \mathcal{F}^n)$ be a linear transformation from $\mathcal{F}^m$ to $\mathcal{F}^n$, and let $\{e_1, \dots, e_m\}$ be the standard basis for $\mathcal{F}^m$. We may uniquely define T by specifying any m vectors $v_1, \dots, v_m$ in $\mathcal{F}^n$. In other words, we define T by the requirement $T(e_i) = v_i$ for each $i = 1, \dots, m$. Since T is linear, for any $x \in \mathcal{F}^m$ we have $x = \sum_{i=1}^m x_ie_i$ and hence

$$T(x) = \sum_{i=1}^m x_iv_i\ .$$

Now define the matrix $A = (a_{ij}) \in M_{n\times m}(\mathcal{F})$ with column vectors given by $A^i = v_i \in \mathcal{F}^n$. In other words (remember these are columns),

$$A^i = (a_{1i}, \dots, a_{ni}) = (v_{1i}, \dots, v_{ni}) = v_i$$

where $v_i = \sum_{j=1}^n f_jv_{ji}$ and $\{f_1, \dots, f_n\}$ is the standard basis for $\mathcal{F}^n$. Writing out T(x) we have

$$T(x) = \sum_{i=1}^m x_iv_i = x_1\begin{pmatrix} v_{11} \\ \vdots \\ v_{n1} \end{pmatrix} + \cdots + x_m\begin{pmatrix} v_{1m} \\ \vdots \\ v_{nm} \end{pmatrix} = \begin{pmatrix} v_{11}x_1 + \cdots + v_{1m}x_m \\ \vdots \\ v_{n1}x_1 + \cdots + v_{nm}x_m \end{pmatrix}$$

and therefore, in terms of the matrix A, our transformation takes the form

$$T(x) = \begin{pmatrix} v_{11} & \cdots & v_{1m} \\ \vdots & & \vdots \\ v_{n1} & \cdots & v_{nm} \end{pmatrix}\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}\ .$$

We have therefore constructed an explicit matrix representation of the transformation T. We shall have much more to say about such matrix representations shortly. //

Given vector spaces U and V, we claim that the set of all linear transformations from U to V can itself be made into a vector space. To accomplish this we proceed as follows. If U and V are vector spaces over F and f, g: U → V are mappings, we naturally define

$$(f + g)(x) = f(x) + g(x)$$

and

$$(cf)(x) = cf(x)$$

for $x \in U$ and $c \in \mathcal{F}$. In addition, if $h: V \to W$ (where W is another vector space over $\mathcal{F}$), then we may define the composite mapping $h \circ g: U \to W$ in the usual way by

$$(h \circ g)(x) = h(g(x)) \;.$$

Theorem 5.2 Let U, V and W be vector spaces over $\mathcal{F}$, let $c \in \mathcal{F}$ be any scalar, and let $f, g: U \to V$ and $h: V \to W$ be linear transformations. Then the mappings $f + g$, cf, and $h \circ g$ are all linear transformations.

Proof First, we see that for $x, y \in U$ and $c \in \mathcal{F}$ we have

$$\begin{aligned}(f+g)(x+y) &= f(x+y)+g(x+y)\\ &= f(x)+f(y)+g(x)+g(y)\\ &= (f+g)(x)+(f+g)(y)\end{aligned}$$

and

$$(f+g)(cx) = f(cx)+g(cx) = cf(x)+cg(x) = c[f(x)+g(x)] = c(f+g)(x)$$

and hence $f + g$ is a linear transformation. The proof that cf is a linear transformation is left to the reader (Exercise 5.1.3). Finally, we see that

$$\begin{aligned}(h\circ g)(x+y) &= h(g(x+y)) = h(g(x)+g(y)) = h(g(x))+h(g(y))\\ &= (h\circ g)(x)+(h\circ g)(y)\end{aligned}$$

and

$$(h\circ g)(cx) = h(g(cx)) = h(cg(x)) = ch(g(x)) = c(h\circ g)(x)$$

so that $h \circ g$ is also a linear transformation. ∎

We define the **zero mapping** $0: U \to V$ by $0x = 0$ for all $x \in U$. Since

$$0(x + y) = 0 = 0x + 0y$$

and

$$0(cx) = 0 = c(0x)$$

it follows that the zero mapping is a linear transformation. Next, given a mapping $f: U \to V$, we define its **negative** $-f: U \to V$ by $(-f)(x) = -f(x)$ for all $x \in U$. If f is a linear transformation, then $-f$ is also linear because cf is linear for any $c \in \mathcal{F}$ and $-f = (-1)f$ (by Theorem 2.1(c)). Lastly, we note that

$$\begin{aligned}[f+(-f)](x) &= f(x)+(-f)(x) = f(x)+[-f(x)] = f(x)+f(-x) = f(x-x)\\ &= f(0) = 0\end{aligned}$$

for all $x \in U$ so that $f + (-f) = (-f) + f = 0$ for all linear transformations f.

With all of this algebra out of the way, we are now in a position to easily prove our claim.

Theorem 5.3 Let U and V be vector spaces over $\mathcal{F}$. Then the set of all linear transformations of U to V with addition and scalar multiplication defined as above is a linear vector space over $\mathcal{F}$.

Proof We leave it to the reader to show that the set of all such linear transformations obeys the properties (V1) – (V8) given in Section 2.1 (see Exercise 5.1.4). ∎

We denote the vector space defined in Theorem 5.3 by L(U, V). (Some authors denote this space by Hom(U, V) since a linear transformation is just a vector space homomorphism). The space L(U, V) is often called the space of **linear transformations** (or **mappings**). In the particular case that U and V are finite-dimensional, we have the following important result.

Theorem 5.4 Let dim U = m and dim V = n. Then

$$\dim L(U, V) = (\dim U)(\dim V) = mn\ .$$

Proof We prove the theorem by exhibiting a basis for L(U, V) that contains mn elements. Let $\{e_1, \ldots, e_m\}$ be a basis for U, and let $\{\bar{e}_1, \ldots, \bar{e}_n\}$ be a basis for V. Define the mn linear transformations $E^i{}_j \in L(U, V)$ by

$$E^i{}_j(e_k) = \delta^i{}_k \bar{e}_j$$

where $i, k = 1, \ldots, m$ and $j = 1, \ldots, n$. Theorem 5.1 guarantees that the mappings $E^i{}_j$ are unique. To show that $\{E^i{}_j\}$ is a basis, we must show that it is linearly independent and spans L(U, V).

If

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a^j{}_i E^i{}_j = 0$$

for some set of scalars $a^j{}_i$, then for any e_k we have

$$0 = \Sigma_{i,\,j} a^j{}_i E^i{}_j(e_k) = \Sigma_{i,\,j} a^j{}_i \delta^i{}_k \bar{e}_j = \Sigma_j a^j{}_k \bar{e}_j\ .$$

But the $\bar{e}_j$ are a basis and hence linearly independent, and thus we must have $a^j{}_k = 0$ for every $j = 1, \ldots, n$ and $k = 1, \ldots, m$. This shows that the $E^i{}_j$ are linearly independent.

Now suppose $f \in L(U, V)$ and let $x \in U$. Then $x = \sum_i x^i e_i$ and

$$f(x) = f(\textstyle\sum_i x^i e_i) = \sum_i x^i f(e_i) \ .$$

Since $f(e_i) \in V$, we must have $f(e_i) = \sum_j c^j{}_i \bar{e}_j$ for some set of scalars $c^j{}_i$, and hence

$$f(e_i) = \textstyle\sum_j c^j{}_i \bar{e}_j = \sum_{j,\,k} c^j{}_k \delta^k{}_i \bar{e}_j = \sum_{j,k} c^j{}_k E^k{}_j (e_i) \ .$$

But this means that $f = \sum_{j,\,k} c^j{}_k E^k{}_j$ (Theorem 5.1), and therefore $\{E^k{}_j\}$ spans $L(U, V)$. ∎

Suppose we have a linear mapping $\phi\colon V \rightarrow \mathcal{F}$ of a vector space V to the field of scalars. By definition, this means that

$$\phi(ax + by) = a\phi(x) + b\phi(y)$$

for every $x, y \in V$ and $a, b \in \mathcal{F}$. The mapping ϕ is called a **linear functional** on V.

Example 5.5 Consider the space $M_n(\mathcal{F})$ of n-square matrices over $\mathcal{F}$. Since the trace of any $A = (a_{ij}) \in M_n(\mathcal{F})$ is defined by

$$\operatorname{Tr} A = \sum_{i=1}^{n} a_{ii}$$

(see Exercise 3.6.7), it is easy to show that Tr defines a linear functional on $M_n(\mathcal{F})$ (Exercise 5.1.5). ////

Example 5.6 Let C[a, b] denote the space of all real-valued continuous functions defined on the interval [a, b] (see Exercise 2.1.6). We may define a linear functional L on C[a, b] by

$$L(f) = \int_a^b f(x)\, dx$$

for every $f \in C[a, b]$. It is also left to the reader (Exercise 5.1.5) to show that this does indeed define a linear functional on C[a, b]. ////

Let V be a vector space over $\mathcal{F}$. Since $\mathcal{F}$ is also a vector space over itself, we may consider the space $L(V, \mathcal{F})$. This vector space is the set of all linear functionals on V, and is called the **dual space** of V (or the **space of linear functionals** on V). The dual space is generally denoted by V*. From the proof of Theorem 5.4, we see that if $\{e_i\}$ is a basis for V, then V* has a unique basis $\{\omega^j\}$ defined by

$$\omega^j(e_i) = \delta^j{}_i \;\; .$$

The basis $\{\omega^j\}$ is referred to as the **dual basis** to the basis $\{e_i\}$. We also see that Theorem 5.4 shows that dim V* = dim V.

(Let us point out that we make no real distinction between subscripts and superscripts. For our purposes, we use whichever is more convenient from a notational standpoint. However, in tensor analysis and differential geometry, subscripts and superscripts are used precisely to distinguish between a vector space and its dual. We shall follow this convention in Chapter 11.)

Example 5.7 Consider the space $V = \mathcal{F}^n$ of all n-tuples of scalars. If we write any $x \in V$ as a column vector, then V* is just the space of row vectors. This is because if $\phi \in V^*$ we have

$$\phi(x) = \phi(\Sigma x_i e_i) = \Sigma x_i \phi(e_i)$$

where the e_i are the standard (column) basis vectors for $V = \mathcal{F}^n$. Thus, since $\phi(e_i) \in \mathcal{F}$, we see that every $\phi(x)$ is the product of some scalar $\phi(e_i)$ times the scalar x_i, summed over i = 1, . . . , n. If we write $\phi(e_i) = a_i$, it then follows that we may write

$$\phi(x) = \phi(x_1, \dots, x_n) = (a_1, \dots, a_n)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad (*)$$

or simply $\phi(x) = \Sigma a_i x_i$. This expression is in fact the origin of the term "linear form."

Since any row vector in $\mathcal{F}^n$ can be expressed in terms of the basis vectors $\omega^1 = (1, 0, \dots, 0), \dots, \omega^n = (0, 0, \dots, 1)$, we see from (*) that the ω^j do indeed form the basis dual to $\{e_i\}$ since they clearly have the property that $\omega^j(e_i) = \delta^j{}_i$. In other words, the row vector ω^j is just the transpose of the corresponding column vector e_j. ∕∕

Since U* is a vector space, the reader may wonder whether or not we may form the space U** = (U*)*. The answer is "yes," and the space U** is called the **double dual** (or **second dual**) of U. In fact, for finite-dimensional vector spaces, it is essentially true that U** = U (in the sense that U and U** are isomorphic). However, we prefer to postpone our discussion of these matters until a later chapter when we can treat all of this material in the detail that it warrants.

Exercises

1. Verify that the mapping T of Theorem 5.1 is well-defined.

2. Repeat Example 5.4, except now let the matrix $A = (a_{ij})$ have row vectors $A_i = v_i \in \mathcal{F}^n$. What is the matrix representation of the operation T(x)?

3. Show that cf is a linear transformation in the proof of Theorem 5.2.

4. Prove Theorem 5.3.

5. (a) Show that the function Tr defines a linear functional on $M_n(\mathcal{F})$ (see Example 5.5).
(b) Show that the mapping L defined in Example 5.6 defines a linear functional.

6. Explain whether or not each of the following mappings f is linear:
(a) $f: \mathbb{R}^2 \to \mathbb{R}$ defined by $f(x, y) = xy$.
(b) $f: \mathbb{R}^2 \to \mathbb{R}$ defined by $f(x, y, z) = 2x - 3y + 4z$.
(c) $f: \mathbb{R}^2 \to \mathbb{R}^3$ defined by $f(x, y) = (x + 1, 2y, x + y)$.
(d) $f: \mathbb{R}^3 \to \mathbb{R}^2$ defined by $f(x, y, z) = (|x|, 0)$.
(e) $f: \mathbb{R}^2 \to \mathbb{R}^2$ defined by $f(x, y) = (x + y, x)$.
(f) $f: \mathbb{R}^3 \to \mathbb{R}^3$ defined by $f(x, y, z) = (1, -x, y + z)$.
(g) $f: \mathbb{R}^2 \to \mathbb{R}^2$ defined by $f(x, y) = (\sin x, y)$.
(h) $f: \mathbb{R}^2 \to \mathbb{R}$ defined by $f(x, y) = |x - y|$.

7. Let $T: U \to V$ be a bijective linear transformation. Define T^{-1} and show that it is also a linear transformation.

8. Let $T: U \to V$ be a linear transformation, and suppose that we have the set of vectors $u_1, \dots, u_n \in U$ with the property that $T(u_1), \dots, T(u_n) \in V$ is linearly independent. Show that $\{u_1, \dots, u_n\}$ is linearly independent.

9. Let $B \in M_n(\mathcal{F})$ be arbitrary. Show that the mapping $T: M_n(\mathcal{F}) \to M_n(\mathcal{F})$ defined by $T(A) = [A, B]_+ = AB + BA$ is linear. Is the same true for the mapping $T'(A) = [A, B] = AB - BA$?

10. Let T: $\mathcal{F}^2 \rightarrow \mathcal{F}^2$ be the linear transformation defined by the system

$$\begin{aligned} y_1 &= -3x_1 + x_2 \\ y_2 &= x_1 - x_2 \end{aligned}$$

and let S be the linear transformation defined by the system

$$\begin{aligned} y_1 &= x_1 + x_2 \\ y_2 &= x_1 \end{aligned}$$

Find a system of equations that defines each of the following linear transformations:

(a) 2T (b) T − S (c) T^2
(d) TS (e) ST (f) $T^2 + 2S$

11. Does there exist a linear transformation T: $\mathbb{R}^3 \rightarrow \mathbb{R}^2$ with the property that T(1, −1, 1) = (1, 0) and T(1, 1, 1) = (0, 1)?

12. Suppose $u_1 = (1, -1)$, $u_2 = (2, -1)$, $u_3 = (-3, 2)$ and $v_1 = (1, 0)$, $v_2 = (0, 1)$, $v_3 = (1, 1)$. Does there exist a linear transformation T: $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ with the property that $Tu_i = v_i$ for each i = 1, 2, and 3?

13. Find T(x, y, z) if T: $\mathbb{R}^3 \rightarrow \mathbb{R}$ is defined by T(1, 1, 1) = 3, T(0, 1, −2) = 1 and T(0, 0, 1) = −2.

14. Let V be the set of all complex numbers considered as a vector space over the real field. Find a mapping T: V → V that is a linear transformation on V, but is not a linear transformation on the space $\mathbb{C}^1$ (i.e., the set of complex numbers considered as a complex vector space).

15. If V is finite-dimensional and $x_1, x_2 \in V$ with $x_1 \neq x_2$, prove there exists a linear functional $f \in V^*$ such that $f(x_1) \neq f(x_2)$.

5.2 FURTHER PROPERTIES OF LINEAR TRANSFORMATIONS

Suppose T ∈ L(U, V) where U and V are finite-dimensional over $\mathcal{F}$. We define the **image** of T to be the set

$$\text{Im } T = \{T(x) \in V: x \in U\}$$

and the **kernel** of T to be the set

$$\text{Ker}\,T = \{x \in U: T(x) = 0\}\ .$$

(Many authors call Im T the **range** of T, but we use this term to mean the space V in which T takes its values.) Since $T(0) = 0 \in V$, we see that $0 \in \text{Im}\,T$, and hence $\text{Im}\,T \neq \varnothing$. Now suppose $x', y' \in \text{Im}\,T$. Then there exist $x, y \in U$ such that $T(x) = x'$ and $T(y) = y'$. Then for any $a, b \in \mathcal{F}$ we have

$$ax' + by' = aT(x) + bT(y) = T(ax + by) \in \text{Im}\,T$$

(since $ax + by \in U$), and thus Im T is a subspace of V. Similarly, we see that $0 \in \text{Ker}\,T$, and if $x, y \in \text{Ker}\,T$ then

$$T(ax + by) = aT(x) + bT(y) = 0$$

so that Ker T is also a subspace of U. Ker T is frequently called the **null space** of T.

We now restate Theorem 2.5 in our current terminology.

Theorem 5.5 A linear transformation $T \in L(U, V)$ is an isomorphism if and only if $\text{Ker}\,T = \{0\}$.

For example, the projection mapping T defined in Example 5.1 is not an isomorphism because $T(0, 0, z) = (0, 0, 0)$ for all $(0, 0, z) \in \mathbb{R}^3$. In fact, if x_0 and y_0 are fixed, then we have $T(x_0, y_0, z) = (x_0, y_0, 0)$ independently of z.

If $T \in L(U, V)$, we define the **rank** of T to be the number

$$r(T) = \dim(\text{Im}\,T)$$

and the **nullity** of T to be the number

$$\text{nul}\,T = \dim(\text{Ker}\,T)\ .$$

We will shortly show that this definition of rank is essentially the same as our previous definition of the rank of a matrix. The relationship between r(T) and nul T is given in the following important result.

Theorem 5.6 If U and V are finite-dimensional over $\mathcal{F}$ and $T \in L(U, V)$, then

$$r(T) + \text{nul}\,T = \dim U\ .$$

Proof Let $\{u_1, \dots, u_n\}$ be a basis for U and suppose that Ker T = {0}. Then for any $x \in U$ we have

$$T(x) = T(\Sigma x_i u_i) = \Sigma x_i T(u_i)$$

for some set of scalars x_i, and therefore $\{T(u_i)\}$ spans Im T. If $\Sigma c_i T(u_i) = 0$, then

$$0 = \Sigma c_i T(u_i) = \Sigma T(c_i u_i) = T(\Sigma c_i u_i)$$

which implies that $\Sigma c_i u_i = 0$ (since Ker T = {0}). But the u_i are linearly independent so that we must have $c_i = 0$ for every i, and hence $\{T(u_i)\}$ is linearly independent. Since nul T = dim(Ker T) = 0 and r(T) = dim(Im T) = n = dim U, we see that r(T) + nul T = dim U.

Now suppose that Ker T ≠ {0}, and let $\{w_1, \dots, w_k\}$ be a basis for Ker T. By Theorem 2.10, we may extend this to a basis $\{w_1, \dots, w_n\}$ for U. Since $T(w_i) = 0$ for each i = 1, . . . , k it follows that the vectors $T(w_{k+1}), \dots, T(w_n)$ span Im T. If

$$\sum_{j=k+1}^{n} c_j T(w_j) = 0$$

for some set of scalars c_i, then

$$0 = \sum_{j=k+1}^{n} c_j T(w_j) = \sum_{j=k+1}^{n} T(c_j w_j) = T(\sum_{j=k+1}^{n} c_j w_j)$$

so that $\Sigma_{j=k+1}^{n} c_j w_j \in$ Ker T. This means that

$$\sum_{j=k+1}^{n} c_j w_j = \sum_{j=1}^{k} a_j w_j$$

for some set of scalars a_i. But this is just

$$\sum_{j=1}^{k} a_j w_j - \sum_{j=k+1}^{n} c_j w_j = 0$$

and hence

$$a_1 = \cdots = a_k = c_{k+1} = \cdots = c_n = 0$$

since the w_j are linearly independent. Therefore $T(w_{k+1}), \dots, T(w_n)$ are linearly independent and thus form a basis for Im T. We have therefore shown that

$$\dim U = k + (n - k) = \dim(\text{Ker } T) + \dim(\text{Im } T) = \text{nul } T + r(T) \ . \ ∎$$

The reader should carefully compare this theorem with Theorem 3.13 and Exercise 3.6.3.

An extremely important special case of the space L(U, V) is the space L(V, V) of all linear transformations of V into itself. This space is frequently written as L(V), and its elements are usually called **linear operators** on V, or simply **operators**.

Recall that Theorem 5.2 showed that the space L(U, V) is closed with respect to addition and scalar multiplication. Furthermore, in the particular case of L(V), the composition of two functions $f, g \in L(V)$ leads naturally to a "multiplication" defined by $fg = f \circ g \in L(V)$. In view of Theorems 5.2 and 5.3, it is now a simple matter to prove the following.

Theorem 5.7 The space L(V) is an associative ring.

Proof All that remains is to verify axioms (R7) and (R8) for a ring as given in Section 1.4. This is quite easy to do, and we leave it to the reader (see Exercise 5.2.1). ∎

In fact, it is easy to see that L(V) is a ring with unit element. In particular, we define the identity mapping $I \in L(V)$ by $I(x) = x$ for all $x \in V$, and hence for any $T \in L(V)$ we have

$$(IT)(x) = I(T(x)) = T(x) = T(I(x)) = (TI)(x)$$

so that I commutes with every member of L(V). (However L(V) is certainly not a commutative ring in general if $\dim V > 1$.)

An associative ring $\mathcal{A}$ is said to be an **algebra** (or **linear algebra**) over $\mathcal{F}$ if $\mathcal{A}$ is a vector space over $\mathcal{F}$ such that

$$a(ST) = (aS)T = S(aT)$$

for all $a \in \mathcal{F}$ and $S, T \in \mathcal{A}$. Another way to say this is that an algebra is a vector space on which an additional operation, called **vector multiplication**, is defined. This operation associates a new vector to each pair of vectors, and is associative, distributive with respect to addition, and obeys the rule $a(ST) = (aS)T = S(aT)$ given above. Loosely put, an algebra is a vector space in which we can also multiply vectors to obtain a new vector. However note, for example, that the space $\mathbb{R}^3$ with the usual "dot product" defined on it does not define an algebra because $\vec{a} \bullet \vec{b}$ is a scalar. Similarly, $\mathbb{R}^3$ with the usual "cross product" is not an algebra because $(\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c})$.

Theorem 5.8 The space L(V) is an algebra over $\mathcal{F}$.

Proof For any $a \in \mathcal{F}$, any $S, T \in L(V)$ and any $x \in V$ we have

$$(a(ST))x = a(ST)(x) = aS(T(x)) = (aS)T(x) = ((aS)T)x$$

and

$$(a(ST))x = aS(T(x)) = S(aT(x)) = S((aT)x) = (S(aT))x\ .$$

This shows that $a(ST) = (aS)T = S(aT)$ and, together with Theorem 5.7, proves the theorem. ∎

A linear transformation $T \in L(U, V)$ is said to be **invertible** if there exists a linear transformation $T^{-1} \in L(V, U)$ such that $TT^{-1} = T^{-1}T = I$ (note that technically TT^{-1} is the identity on V and $T^{-1}T$ is the identity on U). This is exactly the same definition we had in Section 3.7 for matrices. The unique mapping T^{-1} is called the inverse of T.

Theorem 5.9 A linear transformation $T \in L(U, V)$ is invertible if and only if it is a bijection (i.e., one-to-one and onto).

Proof First suppose that T is invertible. If $T(x_1) = T(x_2)$ for $x_1, x_2 \in U$, then the fact that $T^{-1}T = I$ implies

$$x_1 = T^{-1}T(x_1) = T^{-1}T(x_2) = x_2$$

and hence T is injective. If $y \in V$, then using $TT^{-1} = I$ we have

$$y = I(y) = (TT^{-1})y = T(T^{-1}(y))$$

so that $y = T(x)$ where $x = T^{-1}(y)$. This shows that T is also surjective, and hence a bijection.

Conversely, let T be a bijection. We must define a linear transformation $T^{-1} \in L(V, U)$ with the desired properties. Let $y \in V$ be arbitrary. Since T is surjective, there exists a vector $x \in U$ such that $T(x) = y$. The vector x is unique because T is injective. We may therefore define a mapping $T^{-1}: V \to U$ by the rule $T^{-1}(y) = x$ where $y = T(x)$. To show that T^{-1} is linear, let $y_1, y_2 \in V$ be arbitrary and choose $x_1, x_2 \in U$ such that $T(x_1) = y_1$ and $T(x_2) = y_2$. Using the linearity of T we then see that

$$T(x_1 + x_2) = y_1 + y_2$$

and hence

$$T^{-1}(y_1 + y_2) = x_1 + x_2 .$$

But then

$$T^{-1}(y_1 + y_2) = x_1 + x_2 = T^{-1}(y_1) + T^{-1}(y_2) .$$

Similarly, if $T(x) = y$ and $a \in \mathcal{F}$, then $T(ax) = aT(x) = ay$ so that

$$T^{-1}(ay) = ax = aT^{-1}(y) .$$

We have thus shown that $T^{-1} \in L(V, U)$. Finally, we note that for any $y \in V$ and $x \in U$ such that $T(x) = y$ we have

$$TT^{-1}(y) = T(x) = y$$

and

$$T^{-1}T(x) = T^{-1}(y) = x$$

so that $TT^{-1} = T^{-1}T = I$. ∎

A linear transformation $T \in L(U, V)$ is said to be **nonsingular** if Ker T = {0}. In other words, T is nonsingular if it is one-to-one (Theorem 5.5). As we might expect, T is said to be **singular** if it is not nonsingular. In other words, T is singular if Ker T ≠ {0}.

Now suppose U and V are both finite-dimensional and dim U = dim V. If Ker T = {0}, then nul T = 0 and Theorem 5.6 shows that dim U = dim(Im T). In other words, we must have Im T = V, and hence T is surjective. Conversely, if T is surjective then we are forced to conclude that nul T = 0, and thus T is also injective. Hence a linear transformation between two finite-dimensional vector spaces of the same dimension is one-to-one if and only if it is onto. Combining this discussion with Theorem 5.9, we obtain the following result and its obvious corollary.

Theorem 5.10 Let U and V be finite-dimensional vector spaces such that dim U = dim V. Then the following statements are equivalent for any linear transformation $T \in L(U, V)$:

(a) T is invertible.
(b) T is nonsingular.
(c) T is surjective.

Corollary A linear operator $T \in L(V)$ on a finite-dimensional vector space is invertible if and only if it is nonsingular.

Example 5.8 Let V = $\mathcal{F}^n$ so that any x ∈ V may be written in terms of components as x = ($x_1, \ldots, x_n$). Given any matrix A = (a_{ij}) ∈ $M_{m\text{x}n}(\mathcal{F})$, we define a linear transformation T : $\mathcal{F}^n \rightarrow \mathcal{F}^m$ by T(x) = y which is again given in component form by

$$y_i = \sum_{j=1}^{n} a_{ij} x_j \ , \qquad i = 1, \ldots, m \ .$$

We claim that T is one-to-one if and only if the homogeneous system

$$\sum_{j=1}^{n} a_{ij} x_j = 0 \ , \qquad i = 1, \ldots, m$$

has only the trivial solution. (Note that if T is one-to-one, this is the same as requiring that the solution of the nonhomogeneous system be unique. It also follows from Corollary 5 of Theorem 3.21 that if T is one-to-one, then A is nonsingular.)

First let T be one-to-one. Clearly T(0) = 0, and if v = ($v_1, \ldots, v_n$) is a solution of the homogeneous system, then T(v) = 0. But if T is one-to-one, then v = 0 is the only solution. Conversely, let the homogeneous system have only the trivial solution. If T(u) = T(v), then

$$0 = T(u) - T(v) = T(u - v)$$

which implies that u - v = 0 or u = v. //

Example 5.9 Let T ∈ L($\mathbb{R}^2$) be defined by

$$T(x, y) = (y, 2x - y) \ .$$

If T(x, y) = (0, 0), then we must have x = y = 0, and hence Ker T = {0}. By the corollary to Theorem 5.10, T is invertible, and we now show how to find T^{-1}.

Suppose we write (x′, y′) = T(x, y) = (y, 2x - y). Then y = x′ and 2x - y = y′ so that solving for x and y in terms of x′ and y′ we obtain x = (1/2)(x′ + y′) and y = x′. We therefore see that

$$T^{-1}(x', y') = (x'/2 + y'/2, x') \ .$$

Note this also shows that T is surjective since for any (x′, y′) ∈ $\mathbb{R}^2$ we found a point (x, y) = (x′/2 + y′/2, x′) such that T(x, y) = (x′, y′). //

Our next example shows the importance of finite-dimensionality in Theorem 5.10.

Example 5.10 Let V = $\mathcal{F}$[x], the (infinite-dimensional) space of all polynomials over $\mathcal{F}$ (see Example 2.2). For any v ∈ V with v = $\sum^n_{i=0} a_i x^i$ we define T ∈ L(V) by

$$T(v) = \sum_{i=1}^{n} a_i x^{i+1}$$

(this is just a "multiplication by x" operation). We leave it to the reader to show that T is linear and nonsingular (see Exercise 5.2.2). However, it is clear that T can not be surjective (for example, T takes scalars into polynomials of degree 1), so it can not be invertible. However, it is nevertheless possible to find a left inverse T_L^{-1} for T. To see this, we let T_L^{-1} be the operation of subtracting the constant term and then dividing by x:

$$T_L^{-1}(v) = \sum_{i=1}^{n} a_i x^{i-1} \quad .$$

We again leave it to the reader (Exercise 5.2.2) to show that this is a linear transformation, and that $T_L^{-1}T = I$ while $TT_L^{-1} \neq I$.

While the above operation T is an example of a nonsingular linear transformation that is not surjective, we can also give an example of a linear transformation on $\mathcal{F}$[x] that is surjective but not nonsingular. To see this, consider the operation D = d/dx that takes the derivative of every polynomial in $\mathcal{F}$[x]. It is easy to see that D is a linear transformation, but D can not possibly be nonsingular since the derivative of any constant polynomial p(x) = c is zero. Note though, that the image of D is all of $\mathcal{F}$[x], and it is in fact possible to find a right inverse of D. Indeed, if we let $D_R^{-1}(f) = \int_0^x f(t)\, dt$ be the (indefinite) integral operator, then

$$D_R^{-1}\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \frac{a_i x^{i+1}}{i+1}$$

and hence $DD_R^{-1} = I$. However, it is obvious that $D_R^{-1}D \neq I$ because $D_R^{-1}D$ applied to a constant polynomial yields zero. ∕∕

Exercises

1. Finish the proof of Theorem 5.7.

2. (a) Verify that the mapping A in Example 5.8 is linear.
   (b) Verify that the mapping T in Example 5.9 is linear.
   (c) Verify that the mapping T in Example 5.10 is linear and nonsingular.
   (d) Verify that T $T_L^{-1} \neq I$ in Example 5.10.

3. Find a linear transformation T: $\mathbb{R}^3 \rightarrow \mathbb{R}^4$ whose image is generated by the vectors (1, 2, 0, –4) and (2, 0, –1, –3).

4. For each of the following linear transformations T, find the dimension and a basis for Im T and Ker T:
   (a) T: $\mathbb{R}^3 \rightarrow \mathbb{R}^3$ defined by T(x, y, z) = (x + 2y – z, y + z, x + y – 2z).
   (b) T: $\mathbb{R}^4 \rightarrow \mathbb{R}^3$ defined by

$$T(x, y, z, t) = (x - y + z + t, x + 2z - t, x + y + 3z - 3t) \ .$$

5. Consider the space $M_2(\mathbb{R})$ of real 2 x 2 matrices, and define the matrix

$$B = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \ .$$

   Find the dimension and exhibit a specific basis for the kernel of the linear transformation T: $M_2(\mathbb{R}) \rightarrow M_2(\mathbb{R})$ defined by T(A) = AB – BA = [A, B].

6. Let T: U → V be a linear transformation with kernel K_T. If T(u) = v, show that $T^{-1}(v)$ is just the coset u + K_T = {u + k: k ∈ K_T} (see Section 1.5).

7. Show that a linear transformation is nonsingular if and only if it takes linearly independent sets into linearly independent sets.

8. Consider the operator T: $\mathbb{R}^3 \rightarrow \mathbb{R}^3$ defined by

$$T(x, y, z) = (2x, 4x - y, 2x + 3y - z) \ .$$

   (a) Show that T is invertible.
   (b) Find a formula for T^{-1}.

9. Let E be a projection (or idempotent) operator on a space V, i.e., $E^2 = E$ on V. Define U = Im E and W = Ker E. Show that:
   (a) E(u) = u for every u ∈ U.
   (b) If E ≠ I, then E is singular.
   (c) V = U ⊕ W.

10. If S: U → V and T: V → U are nonsingular linear transformations, show that S T is nonsingular. What can be said if S and/or T is singular?

11. Let S: U → V and T: V → W be linear transformations.
(a) Show that T S: U → W is linear.
(b) Show that $r(T S) \le r(T)$ and $r(T S) \le r(S)$, i.e., $r(TS) \le \min\{r(T), r(S)\}$.

12. If S, T ∈ L(V) and S is nonsingular, show that $r(ST) = r(TS) = r(T)$.

13. If S, T ∈ L(U, V), show that $r(S + T) \le r(S) + r(T)$. Give an example of two nonzero linear transformations S, T ∈ L(U,V) such that $r(S + T) = r(S) + r(T)$.

14. Suppose that $V = U \oplus W$ and consider the linear operators E_1 and E_2 on V defined by $E_1(v) = u$ and $E_2(v) = w$ where u ∈ U, w ∈ W and $v = u + w$. Show that:
(a) E_1 and E_2 are projection operators on V.
(b) $E_1 + E_2 = I$.
(c) $E_1E_2 = 0 = E_2E_1$.
(d) $V = \operatorname{Im} E_1 \oplus \operatorname{Im} E_2$.

15. Prove that the nonsingular elements in L(V) form a group.

16. Recall that an operator T ∈ L(V) is said to be **nilpotent** if $T^n = 0$ for some positive integer n. Suppose that T is nilpotent and $T(x) = \alpha x$ for some nonzero x ∈ V and some $\alpha \in \mathcal{F}$. Show that $\alpha = 0$.

17. If dim V = 1, show that L(V) is isomorphic to $\mathcal{F}$.

18. Let $V = \mathbb{C}^3$ have the standard basis $\{e_i\}$, and let T ∈ L(V) be defined by $T(e_1) = (1, 0, i)$, $T(e_2) = (0, 1, 1)$ and $T(e_3) = (i, 1, 0)$. Is T invertible?

19. Let V be finite-dimensional, and suppose T ∈ L(V) has the property that $r(T^2) = r(T)$. Show that $(\operatorname{Im} T) \cap (\operatorname{Ker} T) = \{0\}$.

5.3 MATRIX REPRESENTATIONS

By now it should be apparent that there seems to be a definite similarity between Theorems 5.6 and 3.13. This is indeed the case, but to formulate this relationship precisely, we must first describe the representation of a linear transformation by matrices.

Consider a linear transformation $T \in L(U, V)$, and let U and V have bases $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_m\}$ respectively. Since $T(u_i) \in V$, it follows from Corollary 2 of Theorem 2.4 that there exists a unique set of scalars $a_{1i}, \ldots, a_{mi}$ such that

$$T(u_i) = \sum_{j=1}^{m} v_j a_{ji}$$

for each $i = 1, \ldots, n$. Thus, the linear transformation T leads in a natural way to a matrix (a_{ij}) defined with respect to the given bases. On the other hand, if we are given a matrix (a_{ij}), then $\sum_{j=1}^{m} v_j a_{ji}$ is a vector in V for each $i = 1, \ldots, n$. Hence, by Theorem 5.1, there exists a unique linear transformation T defined by $T(u_i) = \sum_{j=1}^{m} v_j a_{ji}$.

Now let x be any vector in U. Then $x = \sum_{i=1}^{n} x_i u_i$ so that

$$T(x) = T\left(\sum_{i=1}^{n} x_i u_i\right) = \sum_{i=1}^{n} x_i T(u_i) = \sum_{i=1}^{n}\sum_{j=1}^{m} v_j a_{ji} x_i \quad .$$

But $T(x) \in V$ so we may write

$$y = T(x) = \sum_{j=1}^{m} y_j v_j \quad .$$

Since $\{v_i\}$ is a basis for V, comparing these last two equations shows that

$$y_j = \sum_{i=1}^{n} a_{ji} x_i$$

for each $j = 1, \ldots, m$. The reader should note which index is summed over in this expression for y_j.

If we write out both of the systems $T(u_i) = \sum_{j=1}^{m} v_j a_{ji}$ and $y_j = \sum_{i=1}^{n} a_{ji} x_i$, we have

$$\begin{aligned} T(u_1) &= a_{11}v_1 + \cdots + a_{m1}v_m \\ &\vdots \\ T(u_n) &= a_{1n}v_1 + \cdots + a_{mn}v_m \end{aligned} \tag{1}$$

and

$$\begin{aligned} y_1 &= a_{11}x_1 + \cdots + a_{1n}x_n \\ &\vdots \\ y_m &= a_{m1}x_1 + \cdots + a_{mn}x_n \end{aligned} \tag{2}$$

We thus see that the matrix of coefficients in (1) is the transpose of the matrix of coefficients in (2). We shall call the m x n matrix of coefficients in equations (2) the **matrix representation** of the linear transformation T, and we say that T is **represented** by the matrix A = (a_{ij}) with respect to the given (ordered) bases $\{u_i\}$ and $\{v_i\}$.

We will sometimes use the notation [A] to denote the matrix corresponding to an operator $A \in L(U, V)$. This will avoid the confusion that may arise when the same letter is used to denote both the transformation and its representation matrix. In addition, if the particular bases chosen are important, then we will write the matrix representation of the above transformation as $[A]_u^v$, and if $A \in L(V)$, then we write simply $[A]_v$.

In order to make these definitions somewhat more transparent, let us make the following observation. If $x \in U$ has coordinates $(x_1, \dots, x_n)$ relative to a basis for U, and $y \in V$ has coordinates $(y_1, \dots, y_m)$ relative to a basis for V, then the expression $y = A(x)$ may be written in matrix form as $Y = [A]X$ where both X and Y are column vectors. In other words, [A]X is the coordinate vector corresponding to the result of the transformation A acting on the vector x. An equivalent way of writing this in a way that emphasizes the bases involved is

$$[y]_v = [A(x)]_v = [A]_u^v[x]_u \quad .$$

If $\{v_j\}$ is a basis for V, then we may clearly write

$$v_i = \sum_j v_j \delta_{ji}$$

where the δ_{ji} are now to be interpreted as the components of v_i *with respect to the basis* $\{v_j\}$. In other words, v_1 has components $(1, 0, \dots, 0)$, v_2 has components $(0, 1, \dots, 0)$ and so forth. Hence, writing out $[A(u_1)]_v = \sum_{j=1}^m v_j a_{j1}$, we see that

$$[A(u_1)]_v = \begin{pmatrix} a_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_{21} \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ a_{m1} \end{pmatrix} = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}$$

so that $[A(u_1)]_v$ is just the first column of $[A]_u^v$. Similarly, it is easy to see that in general, $[A(u_i)]_v$ is the i*th* column of $[A]_u^v$. In other words, *the matrix representation* $[A]_u^v$ *of a linear transformation* $A \in L(U, V)$ *has columns that are nothing more than the images under* A *of the basis vectors of* U.

We summarize this very important discussion as a theorem for easy reference.

Theorem 5.11 Let U and V have bases $\{u_1, \dots, u_n\}$ and $\{v_1, \dots, v_m\}$ respectively. Then for any $A \in L(U, V)$ the vector

$$[A(u_i)]_v = \sum_{j=1}^{m} v_j a_{ji}$$

is the *ith* column of the matrix $[A]_u^v = (a_{ij})$ that represents A relative to the given bases.

Example 5.11 Let V have a basis $\{v_1, v_2, v_3\}$, and let $A \in L(V)$ be defined by

$$\begin{aligned} A(v_1) &= 3v_1 \qquad\quad + v_3 \\ A(v_2) &= \ \ v_1 - 2v_2 - v_3 \\ A(v_3) &= \qquad\quad v_2 + v_3 \end{aligned}$$

Then the representation of A (relative to this basis) is

$$[A]_v = \begin{pmatrix} 3 & 1 & 0 \\ 0 & -2 & 1 \\ 1 & -1 & 1 \end{pmatrix} . \quad /\!\!/$$

The reader may be wondering why we wrote $A(u_i) = \Sigma_j v_j a_{ji}$ rather than $A(u_i) = \Sigma_j a_{ij} v_j$. The reason is that we want the matrix corresponding to a combination of linear transformations to be the product of the individual matrix representations taken in the same order. (The argument that follows is based on what we learned in Chapter 3 about matrix multiplication, even though technically we have not yet defined this operation within the framework of our current discussion. In fact, our present formulation can be taken as the *definition* of matrix multiplication.)

To see what this means, suppose $A, B \in L(V)$. If we had written (note the order of subscripts) $A(v_i) = \Sigma_j a_{ij} v_j$ and $B(v_i) = \Sigma_j b_{ij} v_j$, then we would have found that

$$\begin{aligned} (AB)(v_i) &= A(B(v_i)) = A(\Sigma_j b_{ij} v_j) = \Sigma_j b_{ij} A(v_j) \\ &= \Sigma_{j,\,k} b_{ij} a_{jk} v_k = \Sigma_k c_{ik} v_k \end{aligned}$$

where $c_{ik} = \Sigma_j b_{ij} a_{jk}$. As a matrix product, we would then have $[C] = [B][A]$. However, if we write (as we did) $A(v_i) = \Sigma_j v_j a_{ji}$ and $B(v_i) = \Sigma_j v_j b_{ji}$, then we obtain

$$\begin{aligned} (AB)(v_i) &= A(B(v_i)) = A(\Sigma_j v_j b_{ji}) = \Sigma_j A(v_j) b_{ji} \\ &= \Sigma_{j,\,k} v_k a_{kj} b_{ji} = \Sigma_k v_k c_{ki} \end{aligned}$$

where now $c_{ki} = \sum_j a_{kj} b_{ji}$. Since the matrix notation for this is [C] = [A][B], we see that the order of the matrix representation of transformations is preserved as desired. We have therefore proven the following result.

Theorem 5.12 For any operators A, B ∈ L(V) we have [AB] = [A][B].

From equations (2) above, we see that any nonhomogeneous system of m linear equations in n unknowns defines an m x n matrix (a_{ij}). According to our discussion, this matrix should also define a linear transformation in a consistent manner.

Example 5.12 Consider the space $\mathbb{R}^2$ with the standard basis

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

so that any $X \in \mathbb{R}^2$ may be written as

$$X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ .$$

Suppose we have the system of equations

$$\begin{aligned} y_1 &= 2x_1 - \ \ x_2 \\ y_2 &= \ \ x_1 + 3x_2 \end{aligned}$$

which we may write in matrix form as [A]X = Y where

$$[A] = \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix} \ .$$

Hence we have a linear transformation A(x) = [A]X. In particular,

$$A(e_1) = \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2e_1 + e_2$$

$$A(e_2) = \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 3 \end{pmatrix} = -e_1 + 3e_2 \ .$$

We now see that letting the *ith* column of [A] be $A(e_i)$, we arrive back at the original form [A] that represents the linear transformation $A(e_1) = 2e_1 + e_2$ and $A(e_2) = -e_1 + 3e_2$. ∕∕

Example 5.13 Consider the space $V = \mathbb{R}^2$ with basis vectors $v_1 = (1, 1)$ and $v_2 = (-1, 0)$. Let T be the linear operator on $\mathbb{R}^2$ defined by

$$T(x, y) = (4x - 2y, 2x + y) \;.$$

To find the matrix of T relative to the given basis, all we do is compute the effect of T on each basis vector:

$$\begin{aligned} T(v_1) &= T(1, 1) = (2, 3) = 3v_1 + v_2 \\ T(v_2) &= T(-1, 0) = (-4, -2) = -2v_1 + 2v_2 \;. \end{aligned}$$

Since the matrix of T has columns given by the image of each basis vector, we must have

$$[T] = \begin{pmatrix} 3 & -2 \\ 1 & 2 \end{pmatrix} \;. \;∕∕$$

Theorem 5.13 Let U and V be vector spaces over $\mathcal{F}$ with bases $\{u_1, \dots, u_n\}$ and $\{v_1, \dots, v_m\}$ respectively. Suppose $A \in L(U, V)$ and let [A] be the matrix representation of A with respect to the given bases. Then the mapping $\phi\colon A \rightarrow [A]$ is an isomorphism of L(U, V) onto the vector space $M_{m\mathrm{x}n}(\mathcal{F})$ of all m x n matrices over $\mathcal{F}$.

Proof Part of this was proved in the discussion above, but for ease of reference, we repeat it here. Given any $(a_{ij}) \in M_{m\mathrm{x}n}(\mathcal{F})$, we define the linear transformation $A \in L(U, V)$ by

$$A(u_i) = \sum_{j=1}^{m} v_j a_{ji}$$

for each $i = 1, \dots, n$. According to Theorem 5.1, the transformation A is uniquely defined and is in L(U, V). By definition, $[A] = (a_{ij})$, and hence ϕ is surjective. On the other hand, given any $A \in L(U, V)$, it follows from Corollary 2 of Theorem 2.4 that for each $i = 1, \dots, n$ there exists a unique set of scalars $a_{1i}, \dots, a_{mi} \in \mathcal{F}$ such that $A(u_i) = \sum_{j=1}^{m} v_j a_{ji}$. Therefore, any $A \in L(U, V)$ has lead to a unique matrix $(a_{ij}) \in M_{m\mathrm{x}n}(\mathcal{F})$. Combined with the previous result that ϕ is surjective, this shows that ϕ is injective and hence a bijection. Another way to see this is to note that if we also have $B \in L(U, V)$ with $[B] = [A]$, then

$$(B-A)(u_i)=B(u_i)-A(u_i)=\sum_{j=1}^{m}v_j(b_{ji}-a_{ji})=0\quad .$$

Since B − A is linear (Theorem 5.3), it follows that (B − A)x = 0 for all x ∈ U, and hence B = A so that ϕ is one-to-one.

Finally, to show that ϕ is an isomorphism we must show that it is also a vector space homomorphism (i.e., a linear transformation). But this is easy if we simply observe that

$$(A+B)(u_i) \;=\; A(u_i)+B(u_i) \;=\; \Sigma_j v_j a_{ji}+\Sigma_j v_j b_{ji} \;=\; \Sigma_j v_j(a_{ji}+b_{ji})$$

and, for any $c \in \mathcal{F}$,

$$(cA)(u_i) \;=\; c(A(u_i)) \;=\; c(\Sigma_j v_j\, a_{ji}) \;=\; \Sigma_j v_j(ca_{ji})\quad .$$

Therefore we have shown that

$$[A+B] \;=\; [A]+[B]$$

and

$$[cA] \;=\; c[A]$$

so that ϕ is a homomorphism. ∎

It may be worth recalling that the space $M_{m\mathrm{x}n}(\mathcal{F})$ is clearly of dimension mn since, for example, we have

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}=a\begin{pmatrix}1&0\\0&0\end{pmatrix}+b\begin{pmatrix}0&1\\0&0\end{pmatrix}+c\begin{pmatrix}0&0\\1&0\end{pmatrix}+d\begin{pmatrix}0&0\\0&1\end{pmatrix}\quad .$$

Therefore Theorem 5.13 provides another proof that dim L(U, V) = mn.

Let us return again to the space L(V) = L(V, V) where dim V = n. In this case, each linear operator A ∈ L(V) will be represented by an n x n matrix, and we then see that the space $M_n(\mathcal{F}) = M_{n\mathrm{x}n}(\mathcal{F})$ of all n x n matrices over $\mathcal{F}$ is closed under addition, multiplication, and scalar multiplication. By Theorem 5.13, L(V) is isomorphic to $M_n(\mathcal{F})$, and this isomorphism preserves addition and scalar multiplication. Furthermore, it also preserves the multiplication of operators since this was the motivation behind how we defined matrix representations (and hence matrix multiplication). Finally, recall that the identity transformation I ∈ L(V) was defined by I(x) = x for all x ∈ V. In particular

$$I(u_i) \;=\; \Sigma_j u_j \delta_{ji}$$

so that the matrix representation of I is just the usual n x n identity matrix that commutes with every other n x n matrix.

Theorem 5.14 The space $M_n(\mathcal{F})$ of all n x n matrices over $\mathcal{F}$ is a linear algebra.

Proof Since $M_n(\mathcal{F})$ is isomorphic to L(V) where dim V = n, this theorem follows directly from Theorem 5.8. ∎

We now return to the relationship between Theorems 5.6 and 3.13. In particular, we would like to know how the rank of a linear transformation is related to the rank of a matrix. The answer was essentially given in Theorem 5.11.

Theorem 5.15 If A ∈ L(U, V) is represented by $[A] = (a_{ji}) \in M_{m \times n}(\mathcal{F})$, then r(A) = r([A]).

Proof Recall that r(A) = dim(Im A) and r([A]) = cr([A]). For any x ∈ U we have

$$A(x) = A(\sum x_i u_i) = \sum x_i A(u_i)$$

so that the $A(u_i)$ span Im A. But $[A(u_i)]$ is just the *ith* column of [A], and hence the $[A(u_i)]$ also span the column space of [A]. Therefore the number of linearly independent columns of [A] is the same as the number of linearly independent vectors in the image of A (see Exercise 5.3.1). This means that r(A) = cr([A]) = r([A]). ∎

Suppose that we have a system of n linear equations in n unknowns written in matrix form as [A]X = Y where [A] is the matrix representation of the corresponding linear transformation A ∈ L(V), and dim V = n. If we are to solve this for a unique X, then [A] must be of rank n (Theorem 3.16). Hence r(A) = n also so that nul A = dim(Ker A) = 0 by Theorem 5.6. But this means that Ker A = {0} and thus A is nonsingular. Note also that Theorem 3.13 now says that the dimension of the solution space is zero (which it must be for the solution to be unique) which agrees with Ker A = {0}.

All of this merely shows the various interrelationships between the matrix nomenclature and the concept of a linear transformation that should be expected in view of Theorem 5.13. Our discussion is summarized by the following useful characterization.

Theorem 5.16 A linear transformation $A \in L(V)$ is nonsingular if and only if $\det [A] \neq 0$.

Proof Let $\dim V = n$. If A is nonsingular then $\text{nul } A = 0$, and hence $r([A]) = r(A) = n$ (Theorem 5.6) so that $[A]^{-1}$ exists (Theorem 3.21). But this means that $\det [A] \neq 0$ (Theorem 4.6). The converse follows by an exact reversal of the argument. ∎

Exercises

1. Suppose $A \in L(U, V)$ and let $\{u_i\}$, $\{v_i\}$ be bases for U and V respectively. Show directly that $\{A(u_i)\}$ is linearly independent if and only if the columns of $[A]$ are also linearly independent.

2. Let V be the space of all real polynomials of degree less than or equal to 3. In other words, elements of V are of the form $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ where each $a_i \in \mathbb{R}$.
   (a) Show that the derivative mapping $D = d/dx$ is an element of $L(V)$.
   (b) Find the matrix of D relative to the ordered basis $\{f_i\}$ for V defined by $f_i(x) = x^{i-1}$.

3. Let $T: \mathbb{R}^3 \to \mathbb{R}^2$ be defined by $T(x, y, z) = (x + y, 2z - x)$.
   (a) Find the matrix of T relative to the standard bases for $\mathbb{R}^3$ and $\mathbb{R}^2$.
   (b) Find the matrix of T relative to the basis $\{\alpha_i\}$ for $\mathbb{R}^3$ and $\{\beta_i\}$ for $\mathbb{R}^2$ where $\alpha_1 = (1, 0, -1)$, $\alpha_2 = (1, 1, 1)$, $\alpha_3 = (1, 0, 0)$, $\beta_1 = (0, 1)$ and $\beta_2 = (1, 0)$.

4. Relative to the standard basis, let $T \in L(\mathbb{R}^3)$ have the matrix representation
$$\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ -1 & 3 & 4 \end{pmatrix}.$$
   Find a basis for $\text{Im } T$ and $\text{Ker } T$.

5. Let $T \in L(\mathbb{R}^3)$ be defined by $T(x, y, z) = (3x + z, -2x + y, -x + 2y + 4z)$.
   (a) Find the matrix of T relative to the standard basis for $\mathbb{R}^3$.
   (b) Find the matrix of T relative to the basis $\{\alpha_i\}$ given by $\alpha_1 = (1, 0, 1)$, $\alpha_2 = (-1, 2, 1)$ and $\alpha_3 = (2, 1, 1)$.

(c) Show that T is invertible, and give a formula for T^{-1} similar to that given in part (a) for T.

6. Let T: $\mathcal{F}^n \rightarrow \mathcal{F}^m$ be the linear transformation defined by

$$T(x_1, \ldots, x_n) = \left(\sum_{i=1}^{n} a_{1i}x_i, \ldots, \sum_{i=1}^{n} a_{mi}x_i \right) .$$

(a) Show that the matrix of T relative to the standard bases of $\mathcal{F}^n$ and $\mathcal{F}^m$ is given by

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} .$$

(b) Find the matrix representation of T: $\mathbb{R}^4 \rightarrow \mathbb{R}^2$ defined by

$$T(x, y, z, t) = (3x - 4y + 2z - 5t, 5x + 7y - z - 2t)$$

relative to the standard bases of $\mathbb{R}^n$.

7. Suppose that T ∈ L(U, V) has rank r. Prove that there exists a basis for U and a basis for V relative to which the matrix of T takes the form

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} .$$

[*Hint*: Show that Ker T has a basis $\{w_1, \ldots, w_{m-r}\}$, and then extend this to a basis $\{u_1, \ldots, u_r, w_1, \ldots, w_{m-r}\}$ for U. Define $v_i = T(u_i)$, and show that this is a basis for Im T. Now extend this to a basis for V.]

8. Let $\{e_i\}$ be the standard basis for $\mathbb{R}^3$, and let $\{f_i\}$ be the standard basis for $\mathbb{R}^2$.

(a) Define T: $\mathbb{R}^3 \rightarrow \mathbb{R}^2$ by $T(e_1) = f_2$, $T(e_2) = f_1$ and $T(e_3) = f_1 + f_2$. Write down the matrix $[T]_e^f$.

(b) Define S: $\mathbb{R}^2 \rightarrow \mathbb{R}^3$ by $S(f_1) = (1, 2, 3)$ and $S(f_2) = (2, -1, 4)$. Write down $[S]_f^e$.

(c) Find $ST(e_i)$ for each i = 1, 2, 3, and write down the matrix $[ST]_e$ of the linear operator ST: $\mathbb{R}^3 \rightarrow \mathbb{R}^3$. Verify that [ST] = [S][T].

9. Suppose T ∈ L(V) and let W be a subspace of V. We say that W is **invariant under** T (or **T-invariant**) if T(W) ⊂ W. If dim W = m, show that T has a block matrix representation of the form

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

where A is an m x m matrix.

10. Let T ∈ L(V), and suppose that V = U ⊕ W where both U and W are T-invariant (see the previous problem). If dim U = m and dim W = n, show that T has a matrix representation of the form

$$\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix}$$

where A is an m x m matrix and B is an n x n matrix.

11. Show that A ∈ L(V) is nonsingular implies $[A^{-1}] = [A]^{-1}$.

5.4 CHANGE OF BASIS

Suppose we have a linear operator A ∈ L(V). Then, given a basis for V, we can write down the corresponding matrix [A]. If we change to a new basis for V, then we will have a new representation for A. We now investigate the relationship between the matrix representations of A in each of these bases.

Given a vector space V, let us consider two arbitrary bases $\{e_1, \dots, e_n\}$ and $\{\bar{e}_1, \dots, \bar{e}_n\}$ for V. Then any vector x ∈ V may be written as either $x = \sum x_i e_i$ or as $x = \sum \bar{x}_i \bar{e}_i$. (It is important to realize that vectors and linear transformations exist independently of the coordinate system used to describe them, and their components may vary from one coordinate system to another.) Since each $\bar{e}_i$ is a vector in V, we may write its components in terms of the basis $\{e_i\}$. In other words, we define the **transition matrix** $[P] = (p_{ij}) \in M_n(\mathcal{F})$ by

$$\bar{e}_i = \sum_{j=1}^{n} e_j p_{ji}$$

for each i = 1, . . . , n. The matrix [P] must be unique for the given bases according to Corollary 2 of Theorem 2.4.

Note that [P] defines a linear transformation P ∈ L(V) by $P(e_i) = \bar{e}_i$. Since $\{P(e_i)\} = \{\bar{e}_i\}$ spans Im P and the $\bar{e}_i$ are linearly independent, it follows that

$r(P) = n$ so that P is nonsingular and hence P^{-1} exists. By Theorem 5.13, we conclude that $[P^{-1}] = [P]^{-1}$. (However, it is also quite simple to show directly that if a linear operator A is nonsingular, then $[A^{-1}] = [A]^{-1}$. See Exercise 5.3.11).

Let us emphasize an earlier remark. From Theorem 5.11, we know that $[\bar{e}_i] = [P(e_i)]$ is just the i*th* column vector of [P]. Since relative to the basis $\{e_i\}$ we have $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0)$ and so on, it follows that the i*th* column of [P] represents the components of $\bar{e}_i$ relative to the basis $\{e_i\}$. In other words, the matrix entry p_{ji} is the j*th* component of the i*th* basis vector $\bar{e}_i$ relative to the basis $\{e_i\}$.

The transition matrix enables us to easily relate the components of any $x \in V$ between the two coordinate systems. To see this, we observe that

$$x = \textstyle\sum_i x_ie_i = \sum_j \bar{x}_j\bar{e}_j = \sum_{i,\,j} \bar{x}_je_ip_{ij} = \sum_{i,\,j} p_{ij}\bar{x}_je_i$$

and hence the uniqueness of the expansion implies $x_i = \sum_j p_{ij}\bar{x}_j$ so that

$$\bar{x}_j = \textstyle\sum_i p^{-1}{}_{ji}x_i \ .$$

This discussion proves the following theorem.

Theorem 5.17 Let [P] be the transition matrix from a basis $\{e_i\}$ to a basis $\{\bar{e}_i\}$ for a space V. Then for any $x \in V$ we have

$$[x]_{\bar{e}} = [P]^{-1}[x]_e$$

which we sometimes write simply as $\bar{X} = P^{-1}X$.

From now on we will omit the brackets on matrix representations unless they are needed for clarity. Thus we will usually write both a linear transformation $A \in L(U, V)$ and its representation $[A] \in M_{m\times n}(\mathcal{F})$ as simply A. Furthermore, to avoid possible ambiguity, we will sometimes denote a linear transformation by T, and its corresponding matrix representation by $A = (a_{ij})$.

Using the above results, it is now an easy matter for us to relate the representation of a linear operator $A \in L(V)$ in one basis to its representation in another basis. If $A(e_i) = \sum_j e_ja_{ji}$ and $A(\bar{e}_i) = \sum_j \bar{e}_j\bar{a}_{ji}$, then on the one hand we have

$$A(\bar{e}_i) = \textstyle\sum_j \bar{e}_j\bar{a}_{ji} = \sum_{j,\,k} e_kp_{kj}\bar{a}_{ji}$$

while on the other hand,

$$A(\bar{e}_i) = A(\textstyle\sum_j e_jp_{ji}) = \sum_j A(e_j)p_{ji} = \sum_{j,\,k} e_ka_{kj}p_{ji} \ .$$

Therefore, since $\{e_k\}$ is a basis for V, we may equate each component in these two equations to obtain $\sum_j p_{kj}\bar{a}_{ji} = \sum_j a_{kj}p_{ji}$ or

$$\bar{a}_{ri} = \sum_{j,\,k} p^{-1}{}_{rk}a_{kj}p_{ji} \quad .$$

In matrix notation, this is just (omitting the brackets on P)

$$[A]_{\bar{e}} = P^{-1}[A]_e P$$

which we will usually write in the form $\bar{A} = P^{-1}AP$ for simplicity.

If $A, B \in M_n(\mathcal{F})$, then B is said to be **similar** to A if there exists a nonsingular matrix S such that $B = S^{-1}AS$, in which case A and B are said to be related by a **similarity transformation**. We leave it to the reader to show that this defines an equivalence relation on $M_n(\mathcal{F})$ (see Exercise 5.4.1).

Since we have shown that in two different bases a linear operator A is represented by two similar matrices, we might wonder whether or not there are any other matrices representing A that are not similar to the others. The answer is given by the following.

Theorem 5.18 If $T \in L(V)$ is represented by A relative to the basis $\{e_i\}$, then a matrix $\bar{A} \in M_n(\mathcal{F})$ represents T relative to some basis $\{\bar{e}_i\}$ if and only if $\bar{A}$ is similar to A. If this is the case, then

$$\bar{A} = P^{-1}AP$$

where P is the transition matrix from the basis $\{e_i\}$ to the basis $\{\bar{e}_i\}$.

Proof The discussion above showed that if A and $\bar{A}$ represent T in two different bases, then $\bar{A} = P^{-1}AP$ where P is the transition matrix from $\{e_i\}$ to $\{\bar{e}_i\}$.

On the other hand, suppose that T is represented by A in the basis $\{e_i\}$, and assume that $\bar{A}$ is similar to A. Then $\bar{A} = P^{-1}AP$ for some nonsingular matrix $P = (p_{ij})$. We define a new basis $\{\bar{e}_i\}$ for V by

$$\bar{e}_i = P(e_i) = \sum_j e_j p_{ji}$$

(where we use the same symbol for both the operator P and its matrix representation). Then

$$T(\bar{e}_i) = T(\textstyle\sum_j e_j p_{ji}) = \sum_j T(e_j)p_{ji} = \sum_{j,\,k} e_k a_{kj} p_{ji}$$

while on the other hand, if T is represented by some matrix $C = (c_{ji})$ in the basis $\{\bar{e}_i\}$, then

$$T(\bar{e}_i) = \Sigma_j \bar{e}_j c_{ji} = \Sigma_{j,\,k} e_k p_{kj} c_{ji} \;.$$

Equating the coefficients of e_k in both of these expressions yields

$$\Sigma_j a_{kj} p_{ji} = \Sigma_j p_{kj} c_{ji}$$

so that

$$c_{ri} = \Sigma_{j,\,k}\, p^{-1}{}_{rk} a_{kj} p_{ji}$$

and hence

$$C = P^{-1}AP = \bar{A} \;.$$

Therefore $\bar{A}$ represents T in the basis $\{\bar{e}_i\}$. ∎

Note that by Theorem 4.8 and its corollary we have

$$\det \bar{A} = \det(P^{-1}AP) = (\det P^{-1})(\det A)(\det P) = \det A$$

and hence all matrices which represent a linear operator T have the same determinant. Another way of stating this is to say that the determinant is **invariant** under a similarity transformation. We thus define the **determinant of a linear operator** $T \in L(V)$ as det A, where A is any matrix representing T.

Another important quantity associated with a matrix $A \in M_n(\mathcal{F})$ is the sum $\Sigma_{i=1}^{n} a_{ii}$ of its diagonal elements. This sum is called the **trace**, and is denoted by Tr A (see Exercise 3.6.7). A simple but useful result is the following.

Theorem 5.19 If $A, B \in M_n(\mathcal{F})$, then $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

Proof We simply compute

$$\begin{aligned}\mathrm{Tr}(AB) &= \Sigma_i (AB)_{ii} = \Sigma_{i,\,j} a_{ij} b_{ji} = \Sigma_j \Sigma_i b_{ji} a_{ij} = \Sigma_j (BA)_{jj}\\ &= \mathrm{Tr}(BA) \;. \;∎\end{aligned}$$

From this theorem it is easy to show that the trace is also invariant under a similarity transformation (see Exercise 4.2.14). Because of this, it also makes sense to speak of the trace of a linear operator.

Example 5.14 Consider the space V = $\mathbb{R}^2$ with its standard basis $e_1 = (1, 0)$ and $e_2 = (0, 1)$, and let $\bar{e}_1 = (1, 2)$, $\bar{e}_2 = (3, -1)$ be another basis. We then see that

$$\begin{aligned}\bar{e}_1 &= e_1 + 2e_2\\ \bar{e}_2 &= 3e_1 - e_2\end{aligned}$$

and consequently the transition matrix P from $\{e_i\}$ to $\{\bar{e}_i\}$ and its inverse P^{-1} are given by

$$P = \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \qquad \text{and} \qquad P^{-1} = \begin{pmatrix} 1/7 & 3/7 \\ 2/7 & -1/7 \end{pmatrix} .$$

Note that P^{-1} may be found either using Theorem 4.11, or by solving for $\{e_i\}$ in terms of $\{\bar{e}_i\}$ to obtain

$$\begin{aligned}e_1 &= (1/7)\bar{e}_1 + (2/7)\bar{e}_2\\ e_2 &= (3/7)\bar{e}_1 - (1/7)\bar{e}_2\end{aligned}$$

Now let T be the operator defined by

$$\begin{aligned}T(e_1) &= (20/7)e_1 - (2/7)e_2\\ T(e_2) &= (-3/7)e_1 + (15/7)e_2\end{aligned}$$

so that relative to the basis $\{e_i\}$ we have

$$A = \begin{pmatrix} 20/7 & -3/7 \\ -2/7 & 15/7 \end{pmatrix} .$$

We thus find that

$$\bar{A} = P^{-1}AP = \begin{pmatrix} 1/7 & 3/7 \\ 2/7 & -1/7 \end{pmatrix}\begin{pmatrix} 20/7 & -3/7 \\ -2/7 & 15/7 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} .$$

Alternatively, we have

$$\begin{aligned}T(\bar{e}_1) &= T(e_1 + 2e_2) = T(e_1) + 2T(e_2) = 2e_1 + 4e_2 = 2\bar{e}_1\\ T(\bar{e}_2) &= T(3e_1 - e_2) = 3T(e_1) - T(e_2) = (63/7)e_1 - 3e_2 = 3\bar{e}_2\end{aligned}$$

so that again we find

$$\bar{A} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} .$$

We now see that

$$\mathrm{Tr}\, A = 20/7 + 15/7 = 5 = \mathrm{Tr}\, \bar{A}$$

and also

$$\det A = 6 = \det \bar{A}$$

as they should. ∕∕

We point out that in this example, $\bar{A}$ turns out to be a diagonal matrix. In this case the basis $\{\bar{e}_i\}$ is said to **diagonalize** the operator T. While it is certainly *not* true that there always exists a basis in which every operator is diagonal, we will spend a considerable amount of time in Chapters 7 and 8 investigating the various standard forms (called **normal** or **canonical**) that a matrix representation of an operator can take.

Let us make one related additional comment about our last example. While it is true that (algebraically speaking) a linear operator is completely determined once its effect on a basis is known, there is no real geometric interpretation of this when the matrix representation of an operator is of the same form as A in Example 5.14. However, if the representation is diagonal as it is with $\bar{A}$, then in this basis the operator represents a magnification factor in each direction. In other words, we see that $\bar{A}$ represents a multiplication of any vector in the $\bar{e}_1$ direction by 2, and a multiplication of any vector in the $\bar{e}_2$ direction by 3. This is the physical interpretation that we will attach to eigenvalues (see Chapter 7).

Exercises

1. Show that the set of similar matrices defines an equivalence relation on $M_n(\mathcal{F})$.

2. Let $\{e_i\}$ be the standard basis for $\mathbb{R}^3$, and consider the basis $f_1 = (1, 1, 1)$, $f_2 = (1, 1, 0)$ and $f_3 = (1, 0, 0)$.
   (a) Find the transition matrix P from $\{e_i\}$ to $\{f_i\}$.
   (b) Find the transition matrix Q from $\{f_i\}$ to $\{e_i\}$.
   (c) Verify that $Q = P^{-1}$.
   (d) Show that $[v]_f = P^{-1}[v]_e$ for any $v \in \mathbb{R}^3$.
   (e) Define $T \in L(\mathbb{R}^3)$ by $T(x, y, z) = (2y + z, x - 4y, 3x)$. Show that $[T]_f = P^{-1}[T]_e P$.

3. Let $\{e_1, e_2\}$ be a basis for V, and define $T \in L(V)$ by $T(e_1) = 3e_1 - 2e_2$ and $T(e_2) = e_1 + 4e_2$. Define the basis $\{f_i\}$ for V by $f_1 = e_1 + e_2$ and $f_2 = 2e_1 + 3e_2$. Find $[T]_f$.

4. Consider the field $\mathbb{C}$ as a vector space over $\mathbb{R}$, and define the linear "conjugation operator" $T \in L(\mathbb{C})$ by $T(z) = z^*$ for each $z \in \mathbb{C}$.
(a) Find the matrix of T relative to the basis $\{e_j\} = \{1, i\}$.
(b) Find the matrix of T relative to the basis $\{f_j\} = \{1 + i, 1 + 2i\}$.
(c) Find the transition matrices P and Q that go from $\{e_j\}$ to $\{f_j\}$ and from $\{f_j\}$ to $\{e_j\}$ respectively.
(d) Verify that $Q = P^{-1}$.
(e) Show that $[T]_f = P^{-1}[T]_e P$.
(f) Verify that $\mathrm{Tr}\,[T]_f = \mathrm{Tr}\,[T]_e$ and $\det [T]_f = \det [T]_e$.

5. Let $\{e_i\}$, $\{f_i\}$ and $\{g_i\}$ be bases for V, and let P and Q be the transition matrices from $\{e_i\}$ to $\{f_i\}$ and from $\{f_i\}$ to $\{g_i\}$ respectively. Show that PQ is the transition matrix from $\{e_i\}$ to $\{g_i\}$.

6. Let A be a 2 x 2 matrix such that only A is similar to itself. Show that A has the form

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} .$$

7. Show that similar matrices have the same rank.

8. Let A, B and C be linear operators on $\mathbb{R}^2$ with the following matrices relative to the standard basis $\{e_i\}$:

$$[A]_e = \begin{pmatrix} 4 & 6 \\ -2 & -3 \end{pmatrix} \qquad [B]_e = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} \qquad [C]_e = \begin{pmatrix} 7 & 3 \\ -10 & -4 \end{pmatrix} .$$

(a) If $f_1 = (2, -1)$ and $f_2 = (3, -2)$, show that $A(f_1) = f_1$ and $A(f_2) = 0$.
(b) Find $[A]_f$.
(c) What is the geometric effect of A?
(d) Show that B is a rotation about the origin of the xy-plane, and find the angle of rotation (see Example 1.2).
(e) If $f_1 = (1, -2)$ and $f_2 = (3, -5)$, find $C(f_1)$ and $C(f_2)$.
(f) Find $[C]_f$.
(g) What is the geometric effect of C?

9. (a) Let $\{e_i\}$ be the standard basis for $\mathbb{R}^n$, and let $\{f_i\}$ be any other orthonormal basis (relative to the standard inner product). Show that the transition matrix P from $\{e_i\}$ to $\{f_i\}$ is **orthogonal**, i.e., $P^T = P^{-1}$.

(b) Let T ∈ L($\mathbb{R}^3$) have the following matrix relative to the standard basis:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 3 \end{pmatrix} .$$

Find the matrix of T relative to the basis f_1 = (2/3, 2/3, −1/3), f_2 = (1/3, −2/3, −2/3) and f_3 = (2/3, −1/3, 2/3).

10. Let T ∈ L($\mathbb{R}^2$) have the following matrix relative to the standard basis $\{e_i\}$ for $\mathbb{R}^2$:

$$[T]_e = \begin{pmatrix} a & b \\ c & d \end{pmatrix} .$$

(a) Suppose there exist two linearly independent vectors f_1 and f_2 in $\mathbb{R}^2$ with the property that $T(f_1) = \lambda_1 f_1$ and $T(f_2) = \lambda_2 f_2$ (where $\lambda_i \in \mathbb{R}$). If P is the transition matrix from the basis $\{e_i\}$ to the basis $\{f_i\}$, show that

$$[T]_f = P^{-1}[T]_e P = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} .$$

(b) Prove there exists a nonzero vector x ∈ $\mathbb{R}^2$ with the property that T(x) = x if and only if

$$\begin{vmatrix} a-1 & b \\ c & d-1 \end{vmatrix} = 0$$

(c) Prove there exists a one-dimensional T-invariant subspace of $\mathbb{R}^2$ if and only if

$$\begin{vmatrix} a-\lambda & b \\ c & d-\lambda \end{vmatrix} = 0$$

for some scalar λ. (Recall that a subspace W is T-invariant if T(W) ⊂ W.)

11. If θ ∈ $\mathbb{R}$, show that the matrices

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

and

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

are similar over the complex field. [*Hint*: Suppose $T \in L(\mathbb{C}^2)$ has the first matrix as its representation relative to the standard basis. Find a new basis $\{v_1, v_2\}$ such that $T(v_1) = \exp(i\theta)v_1$ and $T(v_2) = \exp(-i\theta)v_2$.]

12. Let $V = \mathbb{R}^2$ have basis vectors $e_1 = (1, 1)$ and $e_2 = (1, -1)$. Suppose we define another basis for V by $\bar{e}_1 = (2, 4)$ and $\bar{e}_2 = (3, 1)$. Define the transition operator $P \in L(V)$ as usual by $\bar{e}_i = Pe_i$. Write down the matrix $[P]_e^{\bar{e}}$.

13. Let U have bases $\{u_i\}$ and $\{\bar{u}_i\}$ and let V have bases $\{v_i\}$ and $\{\bar{v}_i\}$. Define the transition operators $P \in L(U)$ and $Q \in L(V)$ by $\bar{u}_i = Pu_i$ and $\bar{v}_i = Qv_i$. If $T \in L(U, V)$, express $[T]_u^v$ in terms of $[T]_{\bar{u}}^{\bar{v}}$.

14. Show that the transition matrix defined by the Gram-Schmidt process is upper-triangular with strictly positive determinant.

Index (Parts I, II, III)